

11/PRTS

09/4464 PCT

420 Rec'd PCT/PTO 20 DEC 1999

1

Beschreibung

## 1. Bezeichnung

- 5 Verfahren und Computersystem zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht

10

## 2. Technischer Hintergrund

german  
applic  
for  
german  
patent

- Es sind verschiedene Netzwerkprotokolle im Bereich des Managements von Rechnernetzen bekannt. Die Aufgaben für die Verwaltung von Rechnernetzen wird durch die hohe Verbreitung von Computern und die immer komplexer werdende Vernetzung von Computern zunehmend schwieriger und die dafür erforderlichen Systeme zum Netzmanagement werden immer mächtiger. Im Rahmen der Verwaltung von Rechnernetzen gewinnt die Frage der Sicherheit des Netzmanagements immer größere Bedeutung. Die Sicherheit des Netzmanagements hängt sehr stark von den in dem System verwendeten Sicherheitstechniken ab.
- 15  
20

- Aus dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 59 - 91, 1994) sind verschiedene Netzwerkprotokolle für das Netzmanagement bekannt, beispielsweise das Simple-Network-Management-Protocol (SNMP) in der Version 1 (SNMPv1) und in der Version 2 (SNMPv2) oder auch das Common-Management-Internet-Protocol (CMIP).
- 25  
30

Das SNMPv1 hat bisher die weiteste Verbreitung zur Überwachung und Kontrolle von Netzwerkkomponenten sowohl über lokale Rechnernetze (Local Area Networks, LANs), als auch bei globalen Netzen (Wide-Area-Networks, WANs).

35

Das SNMPv1 ist im Rahmen des OSI-Kommunikationsschichten-Systems oberhalb der Internetprotokolle User-Datagram-

Protocol (UDP) und Internet-Protocol (IP) angeordnet. Sowohl das UDP als auch das IP weisen erhebliche Schwächen im Bereich der Sicherheit auf, da Sicherheitsmechanismen in diesen Protokollen wenig bis gar nicht integriert sind.

5

Im weiteren werden sowohl das SNMP als auch CMIP als Netzwerkprotokoll bezeichnet.

Die Netzwerkprotokolle werden zur Übertragung von Rechner-  
10. netz-Management-Information zwischen einer ersten Computereinheit, die einen sog. Manager enthält und mindestens einer zweiten Computereinheit, die einen sog. Agenten enthält, verwendet. In einem komplexen Rechnernetz werden üblicherweise mindestens eine Managementstation und eine beliebige Anzahl von von der Managerapplikation überwachten und kontrollierten Rechnern über das Netzwerkprotokoll überwacht bzw.  
15 gesteuert.

Es sind jedoch ebenso Netzwerkmanagementarchitekturen be-  
20 kannt, die mehrere Hierarchien aufweisen, beispielsweise mehrere Computer die von jeweils einem Manager überwacht werden, und mehrere Computer, die jeweils eine Managerapplikation enthalten, die wiederum von einem weiteren Computer, der eine übergeordnete Managerapplikation enthält, überwacht bzw. kontrolliert werden.  
25

Ein Computer, der eine Managerapplikation des jeweiligen Netzwerkprotokolls enthält, wird im weiteren als erste Computereinheit bezeichnet.

30

Jede Computereinheit, die einen Agenten implementiert hat, wird im weiteren als zweite Computereinheit bezeichnet.

Es ist möglich, daß ein Computer sowohl als Manager als auch  
35 als Agent ausgestaltet ist, entsprechend sind die Funktionalitäten in dem Computer enthalten.

Das jeweilige Netzwerkprotokoll kann in dem Computer sowohl in Hardware als auch in Software realisiert sein.

Im weiteren wird von einer einfachen Hierarchie ausgegangen, d.h. es wird nur der Fall beschrieben, bei dem ein erster Computer als Manager eine beliebige Anzahl von zweiten Computern, die Agenten, überwacht, bzw. steuert. Dies dient jedoch lediglich der einfacheren Darstellung. Es ist ohne weiteres möglich, die Erfindung auch in einer Architektur mit einer beliebigen Anzahl von Hierarchieebenen anzuwenden.

Bei den Netzwerkprotokollen wird von der ersten Computereinheit zu den zweiten Computereinheiten entweder eine Informationsabfrage übertragen oder es wird ein Steuerungswert zur Steuerung bzw. Kontrolle der zweiten Computereinheit übertragen.

In jeder zweiten Computereinheit ist es bei den bekannten Netzwerkprotokollen üblich, daß die von der zweiten Computereinheit im Rahmen des Netzwerkprotokolls verwendete Information in Form einer sog. Management-Information-Base (MIB), die die Struktur einer hierarchischen Datenbank aufweist, speichert.

Die Gesamtstruktur der Managementinformation der Netzwerkprotokolle wird in einem sog. globalen Registratur-Baum (Registration-Tree), beispielsweise dem globalen SNMP-Registration-Tree gespeichert. Die MIB eines Agenten, also einer zweiten Computereinheit, ist ein Teil des Registratur-Baums des jeweiligen Netzwerkprotokolls.

Zur Übertragung von Information zwischen der ersten Computereinheit und der zweiten Computereinheit werden digitale Nachrichten, beispielsweise eine SNMPv1-Nachricht verwendet.

Eine SNMPv1-Nachricht enthält eine Versionsnummer, einen sog. Community-String und eine SNMPv1-Protocol-Data-Unit (PDU).

Mit der Versionsnummer wird die Version des verwendeten Netzwerkprotokolls angegeben. Die Versionsnummer wird bei der Implementierung des jeweiligen Netzwerkprotokolls festgelegt.

5

Der Community-String bei der SNMPv1 dient als Passwort für den Zugang zu einer MIB einer zweiten Computereinheit. Der Community-String wird bei SNMPv1 unverschlüsselt zu dem Agenten gesendet. In dem Agenten, also der zweiten Computereinheit, wird überprüft, ob der Community-String, der jeweils zusammen mit einer SNMPv1-Nachricht empfangen wurde, zu einem Zugriff in der MIB der zweiten Computereinheit berechtigt. Da das Passwort bei SNMPv1 unverschlüsselt übertragen wird, ist ein Mißbrauch des Community-Strings leicht möglich, beispielsweise zur Maskierung eines potentiellen Angreifers und zum ungefügten Zugriff auf eine zweite Computereinheit, da es sehr einfach ist für einen potentiellen Angreifer, den Community-String zusammen mit einer IP-Senderadresse eines autorisierten Benutzers abzuhören.

20

SNMPv1 hat somit praktisch keinerlei wirkungsvolle Sicherheitsmechanismen integriert, insbesondere keine wirkungsvolle Authentifikation des SNMPv1-Managers und als Folge der fehlenden Authentifikation keine zuverlässige Zugriffskontrolle auf Seite des Agenten. Ferner enthält SNMPv1 keine Möglichkeit, Sicherheitsmechanismen der Datenintegrität oder der Datenvertraulichkeit zum implementieren. Somit ist es für einen potentiellen Angreifer ohne weiteres möglich, übertragene SNMP-PDUs einfach abzuhören und die übertragene Information zwischen Manager und Agent zu mißbrauchen.

30

Die Codierungsregeln der Netzwerkprotokolle sind detailliert in (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 59 - 91, 1994) beschrieben.

35

Bei der zweiten Version des SNMP, dem SNMPv2 waren zwar verschiedene Sicherheitsmechanismen vorgesehen, jedoch war ins-

besondere die Verwaltung kryptographischer Schlüssel derart aufwendig, daß diese Problematik dazu führte, daß das SNMPv2 trotz erheblicher größerer Möglichkeiten zur Verwaltung von Rechnernetzen verglichen mit SNMPv1, sich gegenüber dem

5 SNMPv1 nicht auf dem Markt durchsetzen konnte. Daher wurde der ursprüngliche SNMPv2 Standard zurückgezogen und durch einen modifizierten Standard, bei dem keine Sicherheit integriert wurde, ersetzt.

- 10 Auch CMIP, das aufgrund allgemein wesentlich größerer Komplexität verglichen mit SNMPv1 und SNMPv2 kaum Berücksichtigung in Produkten gefunden hat, konnte sich auf dem Markt nicht durchsetzen.
- 15 Ferner ist das Konzept von sog. Proxy-Agenten ebenfalls in dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 315, 1994) beschrieben.

### 3. Kurzbeschreibung der Erfindung

20 Somit liegt der Erfindung das Problem zugrunde, Verfahren sowie eine Computersysteme zur Codierung, Übertragung und Decodierung einer digitalen Nachricht anzugeben, bei der kryptographische Sicherheitsmechanismen vorgesehen sind, die einfacher sind als bei den bekannten Verfahren und Anordnungen.

25

Bei dem Verfahren gemäß Patentanspruch 1 wird eine digitale Nachricht, die von der ersten Computereinheit zu der zweiten Computereinheit übertragen werden soll, unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert. Die codierte Nachricht wird mindestens einem kryptographischen Verfahren unterzogen und die kryptographisch bearbeitete codierte Nachricht wird wiederum unter Verwendung des Codierungsformats des Netzwerkprotokolls

30

35 codiert.

Bei dem Verfahren gemäß Patentanspruch 2 wird die Nachricht  
entsprechend dem Codierungsformat des Netzwerkprotokolls de-  
codiert. Ferner wird die decodierte kryptographisch bearbei-  
tete Nachricht einem zu dem mindestens einen kryptographi-  
schen Verfahren inversen kryptographischen Verfahren unterzo-  
gen und die invers kryptographisch bearbeitete Nachricht ent-  
sprechend dem Codierungsformat des Netzwerkprotokolls deco-  
diert.

Bei dem Verfahren gemäß Patentanspruch 3 wird eine digitale  
Nachricht, die von der ersten Computereinheit zu der zweiten  
Computereinheit übertragen werden soll, unter Verwendung ei-  
nes Codierungsformats eines Netzwerkprotokolls zu einer co-  
dierten Nachricht codiert. Die codierte Nachricht wird minde-  
stens einem kryptographischen Verfahren unterzogen und die  
kryptographisch bearbeitete codierte Nachricht wird wiederum  
unter Verwendung des Codierungsformats des Netzwerkprotokolls  
codiert. Nach erfolgter Codierung wird die gesamte Nachricht  
von der ersten Computereinheit mindestens zur zweiten Compu-  
tereinheit übertragen. Die empfangene Nachricht wird in der  
zweiten Computereinheit entsprechend dem Codierungsformat des  
Netzwerkprotokolls decodiert. Anschließend wird die decodier-  
te Nachricht dem zu dem verwendeten kryptographischen Verfah-  
ren inversen kryptographischen Verfahren unterzogen. In einem  
letzten Schritt wird die invers kryptographisch bearbeitete  
Nachricht entsprechend dem Codierungsformat des Netzwerkpro-  
tokolls decodiert.

Durch die "doppelte" Codierung bzw. Decodierung mit dem je-  
weiligen Netzwerkprotokoll wird eine sehr einfache, standard-  
konforme Lösung vorgeschlagen, die Übertragung von Nachrich-  
ten eines Netzwerkprotokolls kryptographisch abzusichern.

Das Verfahren weist ferner den erheblichen Vorteil der einfachen Realisierbarkeit und somit der schnellen Durchführbarkeit mit Hilfe eines Rechners auf.

- 5 Ein weiterer Vorteil ist darin zu sehen, daß die Netzwerkprotokolle unverändert bleiben können und keine neuen Netzwerkprotokolle definiert werden müssen. Somit ist keine aufwendige Versionsumstellung oder gar Neudefinition von Netzwerkprotokollen erforderlich. Die kryptographische Sicherheit des  
10 jeweiligen Netzwerkprotokolls kann ohne größeren Aufwand erheblich erhöht werden.

Das Computersystem gemäß Patentanspruch 12 enthält mindestens  
15 eine Recheneinheit, die derart eingerichtet ist, daß das Verfahren nach einem der Ansprüche 1 bis 11 durchgeführt wird.

Das Computersystem gemäß Patentanspruch 13 zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls, umfaßt mindestens folgende  
20 Komponenten:

- ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht,
- 25 - ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,
- ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.

30

Das Computersystem gemäß Patentanspruch 14 zur Decodierung einer digitalen Nachricht, welches in einem Codierungsformat eines Netzwerkprotokolls vorliegt, umfaßt mindestens folgende Komponenten:

- 35 -- ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,

-- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,

5 -- ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht, und

-- ein achttes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.

10

Das Computersystem gemäß Patentanspruch 15 zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht enthält mindestens folgende

15 Komponenten,

- eine erste Computereinheit, die mindestens folgende Komponenten umfaßt:

-- ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht,

20

-- ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,

-- ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des

25

Netzwerkprotokolls,

-- ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit zu der zweiten Computereinheit,

- eine zweite Computereinheit, die mindestens folgende Komponenten umfaßt:

30

-- ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,

-- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,

35

- ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht, und
- ein achttes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.

Somit weisen die Computersysteme die oben im Zusammenhang mit dem Verfahren beschriebenen Vorteile ebenfalls auf.

10

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

- Besonders vorteilhaft ist das Verfahren im Zusammenhang mit SNMPv1 als Netzwerkprotokoll anwendbar, da für SNMPv1 bisher praktisch keine kryptographische Sicherheit vorhanden ist.

- Doch auch bei den anderen Netzwerkprotokollen kann dieses Verfahren und die entsprechende Anordnung zur Durchführung des Verfahrens verwendet werden, da auch dort die Gesamtkomplexität des jeweiligen Netzwerkprotokolls erheblich reduziert wird.

- Ferner ist es bei dem Computersystem vorteilhaft, ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht, ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls sowie ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht zu der zweiten Computereinheit als einen sog. Proxy-Agenten auszugestalten, der über eine als gesichert angenommene Kommunikationsverbindung zu dem ersten Mittel zur Codierung der digitalen Nachricht unter Verwendung des Netzwerkprotokolls verbunden ist. Der erste Proxy-Agent und die erste Computereinheit können gemeinsam in einer Computereinheit oder auch in zwei unterschiedlichen Computereinheiten realisiert sein.

Auf diese Weise wird unter Verwendung der Proxy-Technik, die aus dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 315, 1994) bekannt ist, die Realisierung eines Computersystems zur kryptographisch sicheren Übertragung von Nachrichten des Codierungsformats eines Netzwerkprotokolls erreicht.

Dieser Vorteil ist ebenso dann gegeben, wenn ein fünftes Mittel zum Empfang der codierten kryptographisch bearbeiteten Nachricht, ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls sowie ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht zusammen in einem zweiten Proxy-Agenten realisiert sind, der über eine als gesichert angenommene Kommunikationsverbindung mit dem Agenten der zweiten Computereinheit unter Verwendung des Netzwerkprotokolls verbunden ist.

#### 4. Kurzbeschreibung der Figuren

20

In den Fig. ist ein Ausführungsbeispiel der Erfindung dargestellt, die im weiteren näher erläutert wird.

Es zeigen

- 25 Fig. 1 ein Ablaufdiagramm, in dem das erfindungsgemäße Verfahren mit Realisierungsdetails für einen Get-Request dargestellt ist;
- Fig. 2 ein Ablaufdiagramm, in dem das Verfahren in seinen Verfahrensschritten mit Realisierungsdetails für einen Set-Request dargestellt ist;
- 30 Fig. 3 ein Ablaufdiagramm, in dem das Verfahren in abstrakter Form dargestellt ist;
- Fig. 4 eine Skizze eines möglichen Aufbaus einer kryptographisch bearbeiteten SNMPv1-Nachricht, in der der Sicherheitsmechanismus der Authentifikation der Originaldaten realisiert wird;
- 35 Fig. 5 der Aufbau einer möglichen kryptographisch bearbei-

teten SNMPv1-Nachricht, mit der die Sicherheitsdienste Integrität und Vertraulichkeit der übertragenen SNMPv1-Nachricht realisiert wird;

Fig. 6 der mögliche Aufbau einer kryptographisch bearbeiteten SNMPv1-Nachricht, in der der Sicherheitsdienst der Vertraulichkeit der SNMPv1-Nachricht realisiert wird;

## 5. Figurenbeschreibung

### Get-Request

In Fig. 1 sind eine erste Computereinheit C1 und eine zweite Computereinheit C2 symbolhaft dargestellt. Die erste Computereinheit C1 weist eine Managerapplikation MA des SNMPv1 sowie einen ersten Proxy-Agenten PA1 auf.

Die zweite Computereinheit C2 weist einen SNMPv1-Agenten AG sowie einen zweiten Proxy-Agenten PA2 auf Seiten der zweiten Computereinheit C2 auf.

In einem ersten Schritt 101 wird in der ersten Computereinheit C1 ein Get-Request gebildet. Unter der Bildung eines Get-Requests ist zu verstehen, daß eine digitale Nachricht unter Verwendung eines Codierungsformats des SNMPv1-Netzwerkprotokolls zu einer codierten Nachricht, dem Get-Request, codiert wird. Dies erfolgt in einem ersten Mittel 101 der ersten Computereinheit C1 zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.

In einem zweiten Schritt 102 wird der Get-Request, d.h. die codierte Nachricht CN von dem ersten Mittel M1 zu dem ersten Proxy-Agenten PA1 auf der Seite der ersten Computereinheit C1 gesendet.

In dem ersten Proxy-Agenten PA1 wird in einem dritten Schritt 103 die codierte Nachricht CN empfangen.

5 In einem vierten Schritt 104 wird die codierte Nachricht CN in dem ersten Proxy-Agenten PA1 mindestens einem kryptographischen Verfahren unterzogen. Zur kryptographischen Bearbeitung der codierten Nachricht in dem vierten Schritt 104 wird ein zweites Mittel 104 eingesetzt.

10 Unter einem kryptographischen Verfahren ist jedes beliebige kryptographische Verfahren z.B. zur Authentifikation, zur Sicherung der Datenintegrität oder auch zur Verschlüsselung von digitalen Daten zu verstehen. Hierbei können beispielsweise das RSA-Verfahren oder auch der Data-Encryption-Standard, der  
15 als DES-Verfahren bezeichnet wird, Verwendung finden.

Als Ergebnis erhält man eine kryptographisch bearbeitete Nachricht KBN, deren Format beispielsweise in den Fig. 3 bis 6 dargestellt ist und im weiteren näher erläutert wird.

20

In einem fünften Schritt 105 wird die kryptographisch bearbeitete Nachricht KBN wiederum unter Verwendung des Codierungsformats des SNMP-Netzwerkprotokolls codiert. Unter diesem Verfahrensschritt ist zu verstehen, daß der kryptographisch bearbeitete Get-Request vorzugsweise in einem Set-Request codiert wird, d.h. eingekapselt wird. Ferner ist ein  
25 drittes Mittel 105 zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls vorgesehen.

30

Wie im weiteren deutlich wird, ist es vorteilhaft, jede Art von Nachricht, die von der ersten Computereinheit C1 zu der zweiten Computereinheit C2 übertragen werden soll, in dem fünften Schritt 105 als Set-Request zu codieren. Dies ist  
35 vorteilhaft, da die Syntax von SNMPv1 für einen Get-Request lediglich Object-Identifiers als zu übertragende Nutzdaten erlaubt. Es ist bei SNMPv1 nicht möglich, die kryptographisch

bearbeitete Information in einem SNMP-Get-Request einzubinden.

5 In einem sechsten Schritt 106 wird der Set-Request als codierte kryptographisch bearbeitete Nachricht CKN von der ersten Computereinheit C1 zu der zweiten Computereinheit C2, d.h. von dem ersten Proxy-Agenten PA1 zu einem zweiten Proxy-Agenten PA2 übertragen.

10 Von dem zweiten Proxy-Agenten PA2 der zweiten Computereinheit C2 wird die codierte kryptographisch bearbeitete Nachricht CKN in einem siebten Schritt 107 empfangen. Hierzu ist ein fünftes Mittel 107 zum Empfangen der codierten kryptographisch bearbeiteten Nachricht CKN vorgesehen.

15 In einem achten Schritt 108 wird von dem zweiten Proxy-Agenten PA2 standardkonform eine Get-Response als Antwort auf den Set-Request an den ersten Proxy-Agenten PA1 der ersten Computereinheit C1 gesendet. Der Get-Response enthält als Bestätigung den jeweiligen Fehlerzustand.

20 In einem neunten Schritt 109 wird die empfangene codierte kryptographisch bearbeitete Nachricht CKN unter Verwendung des Codierungsformats des Netzwerkprotokolls entkapselt, d.h. decodiert. Es ist ein sechstes Mittel 109 zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des SNMPv1-Protokolls vorgesehen.

30 In einem zehnten Schritt 110 wird von dem zweiten Proxy-Agenten PA2 das zu dem jeweils vorgesehenen kryptographischen Verfahren inverse kryptographische Verfahren beispielsweise zur Authentifikation, zur Entschlüsselung bzw. zur Sicherung der Integrität der übertragenen Daten auf die decodierte kryptographisch bearbeitete Nachricht DKN angewendet. Hierzu ist ein siebtes Mittel 110 zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht DKN vorgesehen.

Weiterhin wird die invers kryptographisch bearbeitete Nachricht IKN, d.h. der originale Get-Request, von dem zweiten Proxy-Agenten PA2 zu der Agentenapplikation AG der zweiten  
5 Computereinheit C2 gesendet.

In einem elften Schritt 111 wird der Get-Request von dem Agenten AG empfangen. Hierzu ist ein achttes Mittel 111 Empfangen des Get-Requests vorgesehen.

10

In einem weiteren Schritt 112 wird die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des SNMPv1-Protokolls zu der digitalen Nachricht decodiert, d.h. ausgewertet. Dies bedeutet, daß für den Spezialfall des Get-  
15 Requests die über den Get-Request angeforderte Information eines Werts eines sog. Managed Objects (MO), der in der MIB des Agenten AG gespeichert ist, ausgelesen wird. Die Angabe, welche Information tatsächlich angefordert wird, ist als Object-Identifizier in dem ursprünglichen Get-Request enthalten.

20

Es wird also in dem zwölften Schritt 112 die angeforderte Aktion ausgeführt, in diesem Fall das Auslesen der angeforderten Information, einen Wert eines Managed Objects. Hierzu ist ein neuntes Mittel 112 zur Durchführung der angeforderten Ak-  
25 tion vorgesehen.

Wie es in SNMPv1 vorgesehen ist, wird von dem Agenten AG in der zweiten Computereinheit als Antwort auf einen Get-Request ein Get-Response gebildet und in einem dreizehnten Schritt  
30 113 zu dem zweiten Proxy-Agenten PA2 gesendet. Der Get-Response erhält das Ergebnis der Aktion, die von der ersten Computereinheit C1 in dem Get-Request angefordert wurde.

Der Get-Response wird im weiteren als Antwortnachricht AN bezeichnet.  
35 Die Antwortnachricht AN kann entweder direkt zu der ersten Computereinheit C1 übertragen werden oder, zur weiteren Erhöhung der kryptographischen Sicherheit, entsprechend

dem Codierungsformat des Netzwerkprotokolls noch einmal codiert werden. Es ist in der zweiten Computereinheit C2 ein zehntes Mittel 112 zum Senden des Ergebnisses der Aktion zu der ersten Computereinheit C1 vorgesehen.

5

Weiterhin ist ein elftes Mittel 113 zur Bildung der Antwortnachricht AN vorgesehen, die das Ergebnis der Aktion enthält und zur Codierung der Antwortnachricht AN entsprechend dem Codierungsformat des SNMPv1-Protokolls.

10

In einem vierzehnten Verfahrensschritt 114 wird von dem zweiten Proxy-Agenten PA2 die Antwortnachricht AN empfangen. Hierzu ist ein zwölftes Mittel 114 zum Empfangen der Antwortnachricht AN vorgesehen.

15

In einem fünfzehnten Schritt 115 wird die codierte Antwortnachricht AN mindestens einem kryptographischen Verfahren unterzogen. Hierfür ist ein dreizehntes Mittel 115 zur Bearbeitung der Antwortnachricht AN mit mindestens einem kryptographischen Verfahren vorgesehen. Das Ergebnis dieses Verfahrensschritts ist eine in einem Sicherheitsrahmen eingekapselte Get-Response.

20

Die kryptographisch bearbeitete Antwortnachricht KBAN wird in einer Sicherheits-MIB in dem zweiten Proxy-Agenten PA2 gespeichert (Schritt 116). Der Aufbau der Sicherheits-MIB wird im weiteren detailliert beschrieben.

25

Um die kryptographisch bearbeitete Antwortnachricht KBAN zu erlangen, wird von dem ersten Proxy-Agenten PA1 der ersten Computereinheit C1 ein Get-Request, d.h. eine Abrufnachricht ABN gebildet. Hierfür ist ein vierzehntes Mittel 117 zur Bildung und Codierung der Abrufnachricht ABN entsprechend dem Codierungsformat des SNMPv1-Protokolls vorgesehen, mit der die kryptographisch bearbeitete Antwortnachricht KBAN von der zweiten Computereinheit C2 angefordert wird. Ferner wird die

30

35

codierte Abrufnachricht ABN von der ersten Computereinheit C1 zu der zweiten Computereinheit C2 gesendet.

5 In einem achtzehnten Schritt 118 wird in dem zweiten Proxy-Agenten PA2 die Abrufnachricht ABN, d.h. in diesem Fall der Get-Request, empfangen und standardkonform der übliche Get-Response, der in diesem Fall die kryptographisch bearbeitete Antwortnachricht KBAN enthält, an den ersten Proxy-Agenten PA1 gesendet. Hierzu ist in der zweiten Computereinheit C2  
10 ein fünfzehntes Mittel 118 zum Empfangen der Abrufnachricht ABN und zur Codierung der in der Abrufnachricht ABN angeforderten kryptographisch bearbeiteten Antwortnachricht KBAN entsprechend dem Codierungsformat des SNMPv1-Protokolls, d.h. zur Codierung des angeforderten Get-Response vorgesehen.

15 Die codierte kryptographisch bearbeitete Antwortnachricht wird von dem zweiten Proxy-Agenten PA2 zu dem ersten Proxy-Agenten PA1 übertragen.

20 In einem weiteren Schritt 119 wird in dem ersten Proxy-Agenten PA1 die codierte kryptographisch bearbeitete Antwortnachricht, enthalten in der standardkonformen Get-Response, empfangen. Hierfür ist ein sechzehntes Mittel 119 zum Empfangen der Get-Response in der ersten Computereinheit C1 vorge-  
25 sehen.

In einem weiteren Schritt 120 wird der Get-Request decodiert, d.h. entkapselt und der ursprünglich von dem Agenten AG der zweiten Computereinheit C2 gebildete Get-Response zu der Managerapplikation MA der ersten Computereinheit C1 gesendet.  
30 Hierfür ist ein siebzehntes Mittel 120 vorgesehen zum Decodieren der Get-Response und zum Senden der ursprünglichen, in der Get-Response enthaltenen Get-Response, die die angeforderte Information enthält, zu der Managerapplikation MA.

35 In einem letzten Schritt 121 wird die Get-Response von der Managerapplikation MA empfangen und der angeforderte Wert

ausgewertet und abgespeichert. Hierfür ist ein achtzehntes Mittel 121 zum Empfangen und Auswerten von Managementinformation in der Managerapplikation MA vorgesehen.

- 5 Auf diese Weise wird erreicht, daß ohne großen Mehraufwand und ohne das Verfahren des SNMPv1-Protokolls ändern zu müssen, eine kryptographische Sicherung der Kommunikation möglich wird.

10 **Get-Next-Request**

Für einen Get-Next-Request, der ebenfalls im Rahmen des SNMPv1-Protokolls vorgesehen ist, wird das Verfahren auf die gleiche Weise, wie für den Get-Request beschrieben, durchgeführt, lediglich mit einem veränderten, entsprechend angepaßten Object-Identifizier für den angeforderten Wert des jeweiligen Managed Objects.

**Set-Request**

20

In Fig. 2 ist das Verfahren für einen Set-Request als codierte digitale Nachricht CN dargestellt. Zur einfacheren Erläuterung wird lediglich das Verfahren im weiteren beschrieben, die Mittel sind entsprechend ausgestaltet, daß die einzelnen Verfahrensschritte mit den Computereinheiten C1, C2 durchgeführt werden können.

In einem ersten Schritt 201 wird der Set-Request, d.h. die digitale Nachricht codiert.

30

In einem zweiten Schritt 202 wird von dem Manager MA der ersten Computereinheit der Set-Request, d.h. die codierte Nachricht CN zu dem ersten Proxy-Agenten PA1 gesendet.

35 In einem dritten Schritt 203 wird die codierte Nachricht CN von dem ersten Proxy-Agenten PA1 empfangen.

In einem vierten Schritt 204 wird ein kryptographisches Verfahren auf die codierte Nachricht CN angewendet. Das Ergebnis der kryptographischen Bearbeitung ist eine kryptographisch bearbeitete Nachricht KBN.

5

In einem fünften Schritt 205 wird die kryptographisch bearbeitete Nachricht KBN wiederum unter Verwendung des Codierungsformats des SNMPv1-Protokolls codiert zu einer codierten kryptographisch bearbeiteten Nachricht CKN. Hierfür wird wiederum ein Set-Request verwendet.

10

Der Set-Request wird von dem ersten Proxy-Agenten PA1 zu dem zweiten Proxy-Agenten PA2 gesendet (Schritt 206).

15 In einem siebten Schritt 207 wird von dem zweiten Proxy-Agenten PA2 der Set-Request empfangen.

Als Reaktion auf den Empfang des Set-Requests sendet standardkonform der zweite Proxy-Agent PA2 eine Get-Response, die als Bestätigung den Fehlerzustand enthält (Schritt 208).

20

In einem weiteren Schritt 209 wird die codierte kryptographisch bearbeitete Nachricht decodiert, d.h. "ausgepackt". Das Ergebnis ist die decodierte kryptographisch bearbeitete Nachricht DKN.

25

In einem zehnten Schritt 210 wird jeweils das zu dem verwendeten kryptographischen Verfahren inverse kryptographische Verfahren auf die kryptographisch bearbeitete Nachricht DKN angewendet. Ferner wird die invers kryptographisch bearbeitete Nachricht IKN, d.h. der ursprüngliche Set-Request von dem zweiten Proxy-Agenten PA2 zu dem Agenten AG der zweiten Computereinheit C2 gesendet.

30

35 In einem elften Schritt 211 wird von dem Agenten AG die decodierte kryptographisch bearbeitete Nachricht empfangen und in

einem weiteren Schritt 212 die in dem Set-Request angegebene Aktion durchgeführt.

5 Als Reaktion sendet der Agent AG der zweiten Computereinheit C2 standardkonform die Antwortnachricht AN in Form eines Get-Response zu dem zweiten Proxy-Agenten PA2 (Schritt 213).

In einem vierzehnten Schritt 214 empfängt der zweite Proxy-Agent PA2 die Antwortnachricht AN.

10

In einem fünfzehnten Schritt 215 wird wiederum auf die Antwortnachricht AN mindestens ein vorgebbares kryptographisches Verfahren angewendet.

15 Die weiteren Verfahrensschritte 216, 217, 218, 219, 220 sowie 221 entsprechen den in Zusammenhang mit einem Get-Request beschriebenen Verfahren, den Verfahrensschritten 116, 117, 118, 119, 120 sowie 121.

20 Die Sicherheits-MIB enthält Einträge, die in ihrer Struktur die übliche Syntax zur Beschreibung von Managed-Objects verwendet. Einträgen in der Sicherheits-MIB werden eindeutige Object-Identifiers zugeordnet, die zur eindeutigen Identifizierung der Einträge in der Sicherheits-MIB verwendet werden.

25 Die Object-Identifiers werden in der globalen SNMP-MIB registriert. Damit wird erreicht, daß der Zweck und die Syntax des jeweiligen Managed-Objects bekannt ist. Die verschiedenen Einträge der Sicherheits-MIB können beispielsweise entweder digital unterzeichnete, integritätsgeschützte, oder ver-  
30 schlüsselte Managementinformation enthalten. Selbstverständlich können beliebige Kombinationen der oben beschriebenen Mechanismen in der Sicherheits-MIB eingetragen sein und somit im Rahmen des Verfahrens berücksichtigt werden.

35 Im weiteren wird eine mögliche Beispiel-Syntax in ASN.1 (Abstract Syntax Notation One) einer solchen Sicherheits-MIB dargestellt.

Die Syntax eines sicheren, eingekapselten Managed-Objects ist OCTET STRING. Der Aufbau eines solchen eingekapselten Managed-Objects ist wie folgt:

SecureMO ::=

```
    SEQUENCE {  
        PlainHeader,  
        EncapsulatedData  
5      }
```

PlainHeader ::=

```
    SEQUENCE {  
        SecurityAssociationID,  
10     UsedAlgorithms,  
        AlgorithmParameters  
    }
```

EncapsulatedData ::= OCTET STRING

```
15     -- signed, encrypted, or integrity protected  
     -- ASN.1-encoded data
```

SecurityAssociationID ::= OBJECT IDENTIFIER

20 UsedAlgorithms ::= INTEGER (0..7)

```
    -- value 0 stands for „no security“  
    -- value 1 stands for „signed“  
    -- value 2 stands for „integrity protected“  
    -- value 3 stands for „signed“ and „integrity protected“  
25    -- value 4 stands for „encrypted“  
    -- value 5 stands for „signed“ and „encrypted“  
    -- value 6 stands for „integrity protected“ and  
    --      „encrypted“  
    -- value 7 stands for „signed“, „integrity protected“  
30    --      and „encrypted“
```

AlgorithmParameters ::=

```
    -- necessary parameters for the particular  
    -- algorithms in use  
35
```

Der Wert des Parameters UsedAlgorithms wird nach dem folgenden Schema gebildet. Er kann als Bit-String der Länge 3 Bit repräsentiert werden, wobei das Bit niedrigster Wertigkeit die Verwendung digitaler Signatur („signed“) anzeigt, das Bit mit zweitniedrigster Wertigkeit beispielsweise anzeigt, ob Mechanismen zur Sicherung der Datenintegrität vorgesehen sind („integrity protected“), und das Bit mit der höchsten Wertigkeit beschreibt, ob die Daten verschlüsselt wurden („encrypted“).

Somit kann das Ergebnis jeder kryptographischen Bearbeitung einer Nachricht als ein Bit-String mit der Länge 3 beschrieben werden. Die kryptographisch bearbeitete Nachricht wird als OCTET STRING codiert. Besteht sie aus einer nicht durch 8 teilbaren Anzahl von Bits, so kann sie jedoch durch Anwendung eines sog. Paddings, d.h. durch Auffüllen von Bits ohne semantische Bedeutung, zu einem OCTET STRING erweitert werden.

Diese Situation ist beispielhaft in einem Ablaufdiagramm in Fig. 3 dargestellt.

Ein SNMPv1-Request SR wird gemäß den Vorschriften zur Codierung des jeweiligen Netzprotokolls in ASN.1

(Codierungsregeln, Syntaxdefinition, ER) codiert 301. Der codierte SNMP-Request CSR, d.h. die codierte Nachricht CN wird in einem zweiten Schritt 302 dem jeweiligen kryptographischen Verfahren unterzogen. Hierbei werden beispielsweise kryptographische Schlüssel, Parameter zur Angabe des verwendeten Algorithmus, sowie zusätzliche Information, allgemein kryptographische Information VI, zur Durchführung des jeweiligen kryptographischen Verfahrens verwendet.

Der sich ergebende Bit-String BS wird beispielsweise durch Auffüllen von Füllbits in einem Schritt 303 zu einem OCTET STRING OS konvertiert, z.B. unter Verwendung von Padding PA.

Die abstrakte Vorgehensweise zur inversen kryptographischen Bearbeitung wird entsprechend umgekehrt durchgeführt.

5 Es ist vorteilhaft, existierende Funktionen zur Sicherung der Kommunikation im Rahmen von SNMPv1 dort anzuwenden, wo es möglich ist und diese Sicherheitsfunktionen mit weiteren kryptographischen Verfahren zu verstärken, wo es nötig ist.

10 So ist es vorteilhaft, das Konzept von Community-Strings in SNMPv1 auch im Rahmen dieses Verfahrens zu verwenden. Im Rahmen des Konzepts einer Community werden Gruppen definiert und den einzelnen Gruppen Zugriffsrechte für die jeweiligen Mitglieder der Gruppe zugeordnet. Eine Community und die der Community zugeordneten Zugriffsrechte sind Teil einer Konfi-  
15 guration eines SNMPv1-Agenten. Es ist vorteilhaft, jeweils Communities mit spezifischen Sicherheitsmechanismen zu assoziieren. So ist es beispielsweise möglich, einer Community unterschiedliche kryptographische Algorithmen, kryptographische Schlüssel und entsprechende Parameter, die im Rahmen des  
20 kryptographischen Verfahren jeweils verwendet werden, Mitgliedern der Community zuzuordnen.

Standardkonforme Object-Identifizierer werden vorzugsweise als Angaben verwendet, welche in kryptographischen Verfahren ver-  
25 wendet werden sollen.

Bei der Sicherheitskonfiguration wird vorzugsweise anstelle von kryptographischen Schlüsseln Object-Identifizierer auf gespeicherte kryptographische Schlüssel verwendet, die im wei-  
30 teren als Schlüssel-Identifizierer bezeichnet werden. Durch diese Vorgehensweise wird das jeweilige Schlüsselmaterial besser gesichert.

Weiterhin kann das jeweilige Schlüsselmaterial dadurch stärker  
35 geschützt werden, daß beispielsweise die Dateien, in denen die kryptographischen Schlüssel gehalten werden, verschlüsselt werden oder spezielle Hardwareeinheiten zum Schutz

der kryptographischen Schlüssel vorgesehen sind, beispielsweise Chipkarten.

- Die jeweils zu verwendenden Realisierungsdetails ergeben sich aus der Sicherheitspolitik, die entsprechend der Anwendung stark variieren kann.

### **Authentifikation des Datenursprungs**

- Um den Sicherheitsdienst der Authentifikation der Ursprungsdaten zu erreichen kann beispielsweise folgende Information in der kryptographisch bearbeiteten Nachricht vorgesehen sein (vgl. Fig. 4).
- Der SNMPv1-Request, d.h. die codierte Nachricht CN, wird durch die kryptographische Bearbeitung mit folgenden Header- bzw. Trailer-Informationen umkapselt, wodurch die kryptographisch bearbeitete Nachricht KBN entsteht.
- Ein Authentifikations-Header AH enthält einen Schlüssel-Identifizier KID, mit dem der jeweils zu verwendende kryptographische Schlüssel angegeben ist über einen Object-Identifizier, einen Algorithm-Identifizier AID, mit dem der jeweils zu verwendende kryptographische Algorithmus zur Authentifikation angegeben ist, Algorithmus-Parameter AP, mit denen angegeben wird, welche Parameter im Rahmen der Authentifikation verwendet werden, ein Zeitstempel TS sowie eine Zufallszahl RN.

- Ferner ist als Trailerinformation TI eine digitale Signatur DS vorgesehen. Als Algorithmus zur Authentifikation kann beispielsweise das asymmetrische RSA-Verfahren eingesetzt werden.

### **Zugriffskontrolle für Managementinformation**

35

Die SNMPv1-Zugriffskontrolle basiert auf zwei Mechanismen.

Erstens wird jedem Managed-Object in einer MIB ein Zugriffskontrollwert zugeordnet, der einen der drei folgenden Werte aufweist:

- Read-Only,
- 5 - Read-Write,
- Write-Only,
- Not-Accessable.

Zweitens wird jeder Community in dem SNMPv1-Agentenkonfiguration ein sog. MIB-View zusammen mit den jeweiligen Zugriffsrechten zugeordnet. Ein MIB-View enthält eine vorgebbare Anzahl von Object-Identifiern, die die jeweiligen Unterbäume oder sog. Blätter des SNMP-Registratur-Baums bezeichnen.

Die jeweiligen Zugriffsrechte weisen einen der folgenden Werte auf:

- Read Only,
- Write-Only,
- 20 - Read-Write,
- None.

#### **Sicherung der Datenintegrität eines SNMP-Requests**

Zur Sicherung der Datenintegrität wird ein Mechanismus zur kryptographischen Sicherung der Datenintegrität eingesetzt. Hierfür werden Datenintegritätsprüfsummen über den gesamten SNMPv1-Request oder einen Teil davon gebildet. Dies kann beispielsweise mittels des DES im sog. Cipher-Block-Chaining-Mode (CBC-Modus) erfolgen. Für diesen speziellen Mechanismus ist die Verwendung eines 64 Bit langen Initialisierungswerts erforderlich, der jeder Partei der jeweiligen Sicherheitsgruppe bekannt sein muß. Der Initialisierungswert ist Teil der Algorithmusparameter AP, die in der Header-Information HI der kryptographisch bearbeiteten Nachricht KBN verwendet wird (vgl. Fig. 5). Ferner weist die Header-Information HI einen Schlüssel-Identifizier KID sowie einen Algorithmus-Identifizier

AID auf, deren Funktionalität gleich ist wie bei der Authentifikation.

5 Ferner ist in einer Trailer-Information TI ein Integritätsprüfwert ICV vorgesehen.

### **Verschlüsselung von SNMPv1-Requests**

10 Vertraulichkeit der übertragenen SNMPv1-Daten kann auf ähnliche Weise erfolgen, wie die Sicherung der Datenintegrität. Zur Verschlüsselung kann beispielsweise wiederum das DES-Verfahren im CBC-Modus verwendet werden. In diesem Fall ist wiederum ein Initialisierungswert als Algorithmusparameter AP und einer Header-Information HI der kryptographisch bearbeiteten Nachricht KBN erforderlich (vgl. Fig. 6).

20 Wiederum ist in der Header-Information HI ein Schlüssel-Identifizier KID sowie ein Algorithmus-Identifizier AID mit oben beschriebener Funktionalität vorgesehen.

Weiterhin können Mechanismen zur Protokollierung der Kommunikation sowie zur Alarmgebung bei Auffinden von Angriffsversuchen vorgesehen sein.

25 Das Verfahren und das Computersystem können sehr vorteilhaft im Rahmen eines Szenarios verwendet werden, bei dem ein Anbieter eines Kommunikationsnetzes Bandbreite des Kommunikationsnetzes einem Dienstanbieter zur Verfügung stellt, der Dritten zusätzliche Dienste zur Verfügung stellt, die das  
30 Kommunikationsnetz als solche nicht vorsieht. In diesem Zusammenhang kann das Verfahren sowie das Computersystem vorteilhaft beispielsweise zur Kontrolle oder auch zur Abrechnung der von dem Anbieter des gesamten Kommunikationsnetzes zur Verfügung gestellten Ressourcen dienen. In diesem Fall  
35 wird der Manager auf einem Computer des Anbieters des gesamten Kommunikationsnetzes realisiert sein und ein Agent jeweils bei dem Anbieter zusätzlicher Dienste.

In einer Variante des oben beschriebenen Ausführungsbeispiels ist es vorgesehen, die Antwortnachricht direkt, ohne Warten auf eine Abrufnachricht, zu codieren und an die erste Computereinheit zu senden. Somit sind folgende Schritte in der

- die Codierung einer Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls in der ersten Computereinheit, mit der die kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit angefordert wird,
- die Übertragung der Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit, sowie
- das Empfangen der Abrufnachricht.

Entsprechendes gilt für das Computersystem.

Anschaulich kann das Verfahren derart beschrieben werden, daß zu dem standardkonformen Netzwerkprotokoll z.B. dem SNMPv1-Protokoll auf den jeweiligen SNMP-Request oder auch CMIP-Request, ein kryptographisches Verfahren angewendet wird, mit dem eine kryptographische Sicherung des SNMP-Requests bzw. dem CMIP-Request erreicht wird. Um jedoch die Verwendung standardkonformer SNMP-Verfahren zu ermöglichen, wird die kryptographisch bearbeitete Nachricht wiederum mit dem jeweiligen Codierungsformat des Netzwerkprotokolls codiert. Dies entspricht einer "doppelten" Anwendung des jeweiligen Netzwerkprotokolls auf die zu codierende Nachricht.

## Patentansprüche

1. Verfahren zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls,

- 5 - bei dem die Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht codiert wird,  
- bei dem die codierte Nachricht mindestens einem kryptographischen Verfahren unterzogen wird, und  
10 - bei dem die kryptographisch bearbeitete Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls codiert wird.

2. Verfahren zur Decodierung einer digitalen Nachricht, welches in einem Codierungsformat eines Netzwerkprotokolls vorliegt,

- 15 - bei dem die Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert wird,  
- bei dem die decodierte kryptographisch bearbeitete Nachricht einem zu dem mindestens einen kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen wird, und  
20 - bei dem die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert wird.

25 3. Verfahren zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht,

- 30 - bei dem in der ersten Computereinheit folgende Schritte durchgeführt werden:  
-- die Nachricht wird unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert,  
35 -- die codierte Nachricht wird mindestens einem kryptographischen Verfahren unterzogen wird,

- die kryptographisch bearbeitete Nachricht wird unter Verwendung des Codierungsformats des Netzwerkprotokolls codiert,
- bei dem die codierte kryptographisch bearbeitete Nachricht von der ersten Computereinheit zu der zweiten Computereinheit  
5 übertragen wird,
- bei dem in der zweiten Computereinheit folgende Schritte durchgeführt werden:
  - die empfangene Nachricht wird entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert,
  - 10 - die decodierte kryptographisch bearbeitete Nachricht wird einem zu dem mindestens einen kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen, und
  - die invers kryptographisch bearbeitete Nachricht wird entsprechend dem Codierungsformat des Netzwerkprotokolls zu der  
15 digitalen Nachricht decodiert.

4. Verfahren nach Anspruch 3,
- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
  - 20 - bei dem in der zweiten Computereinheit die angeforderte Aktion ausgeführt wird, und
  - bei dem in der zweiten Computereinheit das Ergebnis der Aktion in einer Antwortnachricht zu der ersten Computereinheit gesendet wird.

- 25 5. Verfahren nach Anspruch 3,
- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
  - bei dem in der zweiten Computereinheit die angeforderte Aktion  
30 ausgeführt wird,
  - bei dem in der zweiten Computereinheit eine Antwortnachricht gebildet wird, die ein Ergebnis der Aktion enthält,
  - bei dem in der zweiten Computereinheit die Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls co-  
35 diert wird,
  - bei dem in der zweiten Computereinheit die Antwortnachricht mindestens einem kryptographischen Verfahren unterzogen wird,

5  
- bei dem in der zweiten Computereinheit die kryptographisch bearbeitete Antwortnachricht gespeichert wird,

- bei dem in der ersten Computereinheit eine Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, mit der die kryptographisch bearbeitete Antwort-

nachricht von der zweiten Computereinheit angefordert wird, - bei dem die Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit übertragen wird, .

- bei dem die Abrufnachricht von der zweiten Computereinheit empfangen wird,

- bei dem die kryptographisch bearbeitete Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, und

- bei dem die codierte kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit übertragen wird.

6. Verfahren nach Anspruch 3,

- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,

- bei dem in der zweiten Computereinheit die angeforderte Aktion ausgeführt wird,

- bei dem in der zweiten Computereinheit eine Antwortnachricht gebildet wird, die ein Ergebnis der Aktion enthält,

- bei dem in der zweiten Computereinheit die Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird,

- bei dem in der zweiten Computereinheit die Antwortnachricht mindestens einem kryptographischen Verfahren unterzogen wird,

- bei dem die kryptographisch bearbeitete Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, und

- bei dem die codierte kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit übertragen wird.

7. Verfahren nach einem der Ansprüche 2 bis 6,

bei dem in der zweiten Computereinheit die kryptographisch bearbeitete Antwortnachricht in einer Management Information Base (MIB) gespeichert wird.

- 5 8. Verfahren nach einem der Ansprüche 1 bis 4,  
bei dem als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird.

9. Verfahren nach Anspruch 8,  
10 - bei dem in der ersten Computereinheit bei der Codierung der kryptographisch bearbeiteten Nachricht ein Set-Request gebildet wird, und  
- bei dem der Set-Request von der ersten Computereinheit zu der zweiten Computereinheit übertragen wird.

- 15 10. Verfahren nach Anspruch 8 oder 9,  
- bei dem als Abrufnachricht ein Get-Request verwendet wird,  
- bei dem bei der Codierung der angeforderten kryptographisch bearbeiteten Antwortnachricht ein Get-Response gebildet wird.

- 20 11. Verfahren nach einem der Ansprüche 4 bis 10,  
bei dem als Aktion eine Informationsabfrage und/oder eine Informationsangabe der zweiten Computereinheit übertragen wird.

- 25 12. Vorrichtung mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß das Verfahren nach einem der Ansprüche 1 bis 11 durchführbar ist.

- 30 13. Vorrichtung zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls, das mindestens folgende Komponenten umfaßt:  
- ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht,  
35 - ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,

- ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.

- 5 14. Vorrichtung zur Decodierung einer digitalen Nachricht, welches in einem Codierungsformat eines Netzwerkprotokolls vorliegt, das mindestens folgende Komponenten umfaßt:
- ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,
  - 10 -- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
  - ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht,
  - 15 und
  - ein achttes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.
- 20 15. Vorrichtung zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht,
- bei dem eine erste Computereinheit vorgesehen ist, die mindestens folgende Komponenten umfaßt:
  - 25 -- ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht,
  - ein zweites Mittel zur kryptographischen Bearbeitung der
  - 30 codierten Nachricht,
  - ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls,
  - ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit
  - 35 zu der zweiten Computereinheit,

- bei dem eine zweite Computereinheit vorgesehen ist, die mindestens folgende Komponenten umfaßt:

-- ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,

5 -- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,

-- ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht,  
10 und

-- ein achttes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.

15 16. Vorrichtung nach Anspruch 13 oder 15,  
bei dem als drittes Mittel das erste Mittel vorgesehen ist.

17. Vorrichtung nach Anspruch 14 oder 15,  
bei dem als achttes Mittel das sechste Mittel vorgesehen ist.

20 18. Vorrichtung nach einem der Ansprüche 15 bis 17,  
- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,  
- bei dem in der zweiten Computereinheit ein neuntes Mittel  
25 zur Durchführung der angeforderten Aktion vorgesehen ist, und  
- bei dem in der zweiten Computereinheit ein zehntes Mittel zum Senden des Ergebnisses der Aktion zu der ersten Computereinheit vorgesehen ist.

30 19. Vorrichtung nach einem der Ansprüche 15 bis 18,  
- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,  
- bei dem in der zweiten Computereinheit ein neuntes Mittel zur Durchführung der angeforderten Aktion vorgesehen ist,  
35 - bei dem in der zweiten Computereinheit ein elftes Mittel zur Bildung einer Antwortnachricht, die ein Ergebnis der Aktion enthält, vorgesehen ist,

- bei dem in der zweiten Computereinheit ein zwölftes Mittel zur Codierung Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
- bei dem in der zweiten Computereinheit ein dreizehntes Mittel zur Bearbeitung der Antwortnachricht mit mindestens einem kryptographischen Verfahren vorgesehen ist,
- bei dem in der zweiten Computereinheit ein vierzehntes Mittel zur Speicherung der kryptographisch bearbeiteten Antwortnachricht vorgesehen ist,
- 10 - bei dem in der ersten Computereinheit ein fünfzehntes Mittel zur Bildung und Codierung einer Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, mit der die kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit angefordert wird, vorgesehen ist,
- 15 - bei dem in der ersten Computereinheit ein sechzehntes Mittel zum Senden der Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit, vorgesehen ist,
- bei dem in der zweiten Computereinheit ein siebzehntes Mittel zum Empfangen der Abrufnachricht vorgesehen ist
- 20 - bei dem in der zweiten Computereinheit ein achtzehntes Mittel zur Codierung der in der Abrufnachricht angeforderten kryptographisch bearbeiteten Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, vorgesehen ist, und
- 25 - bei dem in der zweiten Computereinheit ein neunzehntes Mittel zum Senden der codierten kryptographisch bearbeiteten Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit, vorgesehen ist.
- 30 20. Vorrichtung nach einem der Ansprüche 15 bis 18,
  - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
  - bei dem in der zweiten Computereinheit ein neuntes Mittel zur Durchführung der angeforderten Aktion vorgesehen ist,
  - 35 - bei dem in der zweiten Computereinheit ein elftes Mittel zur Bildung einer Antwortnachricht, die ein Ergebnis der Aktion enthält, vorgesehen ist,

- bei dem in der zweiten Computereinheit ein zwölftes Mittel zur Codierung Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
  - bei dem in der zweiten Computereinheit ein dreizehntes Mittel zur Bearbeitung der Antwortnachricht mit mindestens einem kryptographischen Verfahren vorgesehen ist,
  - bei dem in der zweiten Computereinheit ein achtzehntes Mittel zur Codierung der kryptographisch bearbeiteten Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, vorgesehen ist, und
  - bei dem in der zweiten Computereinheit ein neunzehntes Mittel zum Senden der codierten kryptographisch bearbeiteten Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit, vorgesehen ist.
21. Vorrichtung nach Anspruch 19 oder 20, bei dem das vierzehnte Mittel derart ausgestaltet ist, daß die kryptographisch bearbeitete Antwortnachricht in einer Management Information Base (MIB) gespeichert wird.
22. Vorrichtung nach einem der Ansprüche 13 bis 21, das derart ausgestaltet ist, daß als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird.
23. Vorrichtung nach Anspruch 13 oder 15,
- das derart ausgestaltet ist, daß als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird, und
  - bei dem das dritte Mittel zur Codierung der kryptographisch bearbeiteten Nachricht derart ausgestaltet ist, daß bei der Codierung der kryptographisch bearbeiteten Nachricht ein Set-Request gebildet wird.
24. Vorrichtung nach Anspruch 22,

- bei dem das fünfzehnte Mittel zur Bildung und Codierung der Abrufnachricht derart ausgestaltet ist, daß ein Get-Request gebildet wird,

- 5 - bei dem das achtzehnte Mittel zur Codierung der in der Abrufnachricht angeforderten kryptographisch bearbeiteten Antwortnachricht derart ausgestaltet ist, daß ein Get-Response gebildet wird.

25. Vorrichtung nach einem der Ansprüche 15 bis 24,  
10 bei dem als Aktion eine Informationsabfrage und/oder eine Informationsangabe der zweiten Computereinheit vorgesehen ist.

26. Vorrichtung nach einem der Ansprüche 12 bis 25,  
bei dem das zweite Mittel, das dritte Mittel und das vierte  
15 Mittel zusammen als ein erster Proxy Agent ausgestaltet sind, und/oder  
bei dem das fünfte Mittel, das sechste Mittel und das siebte Mittel zusammen als ein zweiter Proxy Agent ausgestaltet sind.

20

27. Kommunikationssystem mit einem Managers eines Kommunikationsnetzes und eines Zwischenmanagers eines Kommunikationsnetzes, der das Kommunikationsnetz verwendet und weitere  
Dienste, die über die von dem Kommunikationsnetz angebotenen  
25 Dienste hinausgehen, Kunden anbietet mit einem Computersystem nach einem der Ansprüche 13 bis 26.

## Zusammenfassung

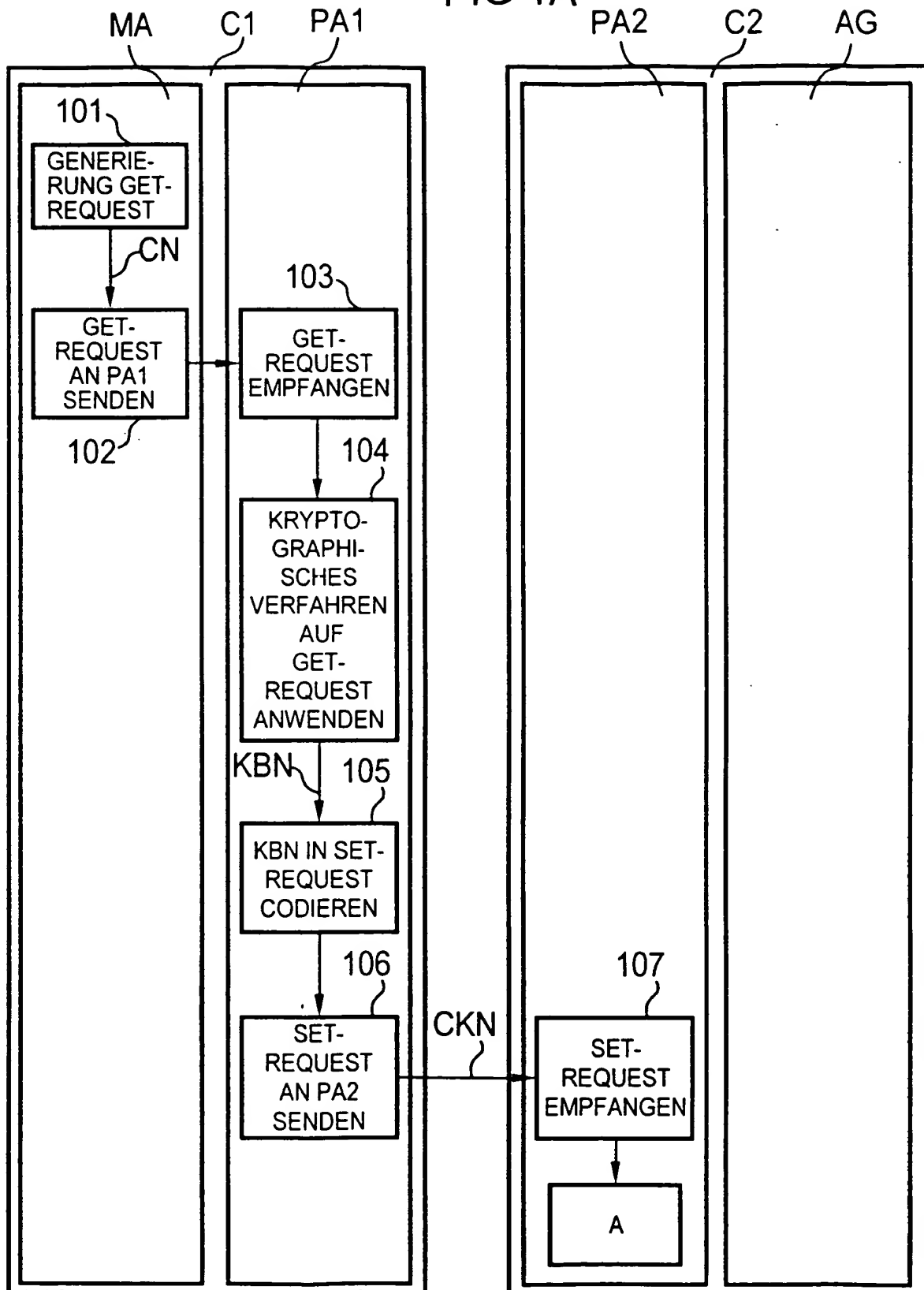
Verfahren und Computersystem zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten  
5 Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht

Es wird ein Verfahren vorgestellt, bei dem für ein Netzwerk-  
protokoll, z.B. für das SNMPv1, wird in der ersten Compu-  
10 tereinheit (C1) eine Nachricht unter Verwendung des Codie-  
rungsformats des Netzwerkprotokolls zu einer codierten Nach-  
richt (CN) codiert (101). Die codierte Nachricht (CN) wird  
einem kryptographischen Verfahren unterzogen (104). Die da-  
durch gebildete kryptographisch bearbeitete Nachricht (KBN)  
15 wird wiederum unter Verwendung des Codierungsformats des  
Netzwerkprotokolls codiert (105). Die auf diese Weise codier-  
te kryptographisch bearbeitete Nachricht (CKN) wird von der  
ersten Computereinheit (C1) zu der zweiten Computereinheit  
(C2) übertragen. In der zweiten Computereinheit (C2) wird die  
20 empfangene Nachricht entsprechend dem Codierungsformat des  
Netzwerkprotokolls decodiert (109) und es wird ein inverses  
kryptographisches Verfahren (110) auf die decodierte Nach-  
richt (DKN) angewendet. Die invers kryptographisch bearbeite-  
te Nachricht (IKN) wird entsprechend dem Codierungsformat des  
25 Netzwerkprotokolls wiederum decodiert.

Sig. Fig. 1

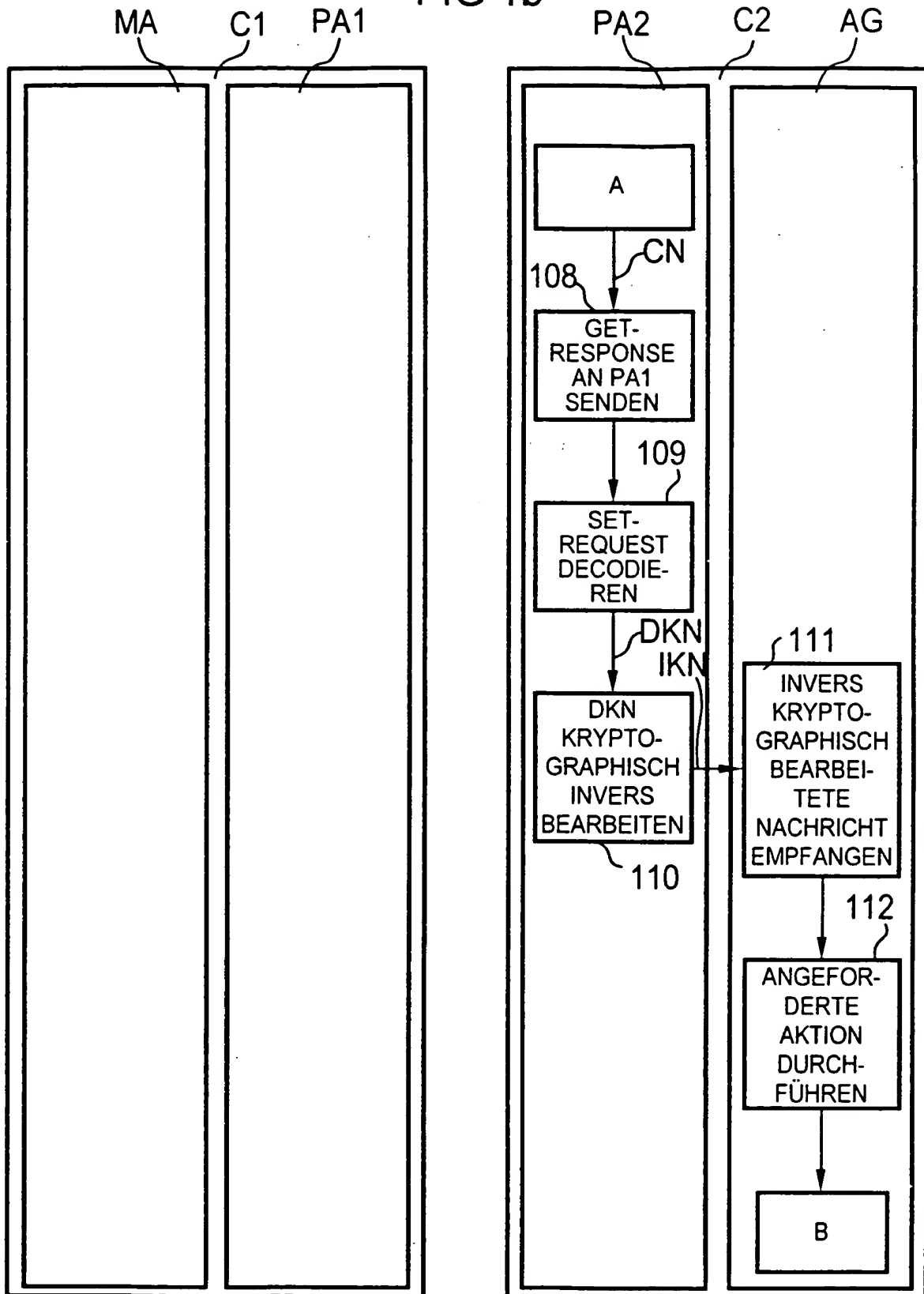
1/11

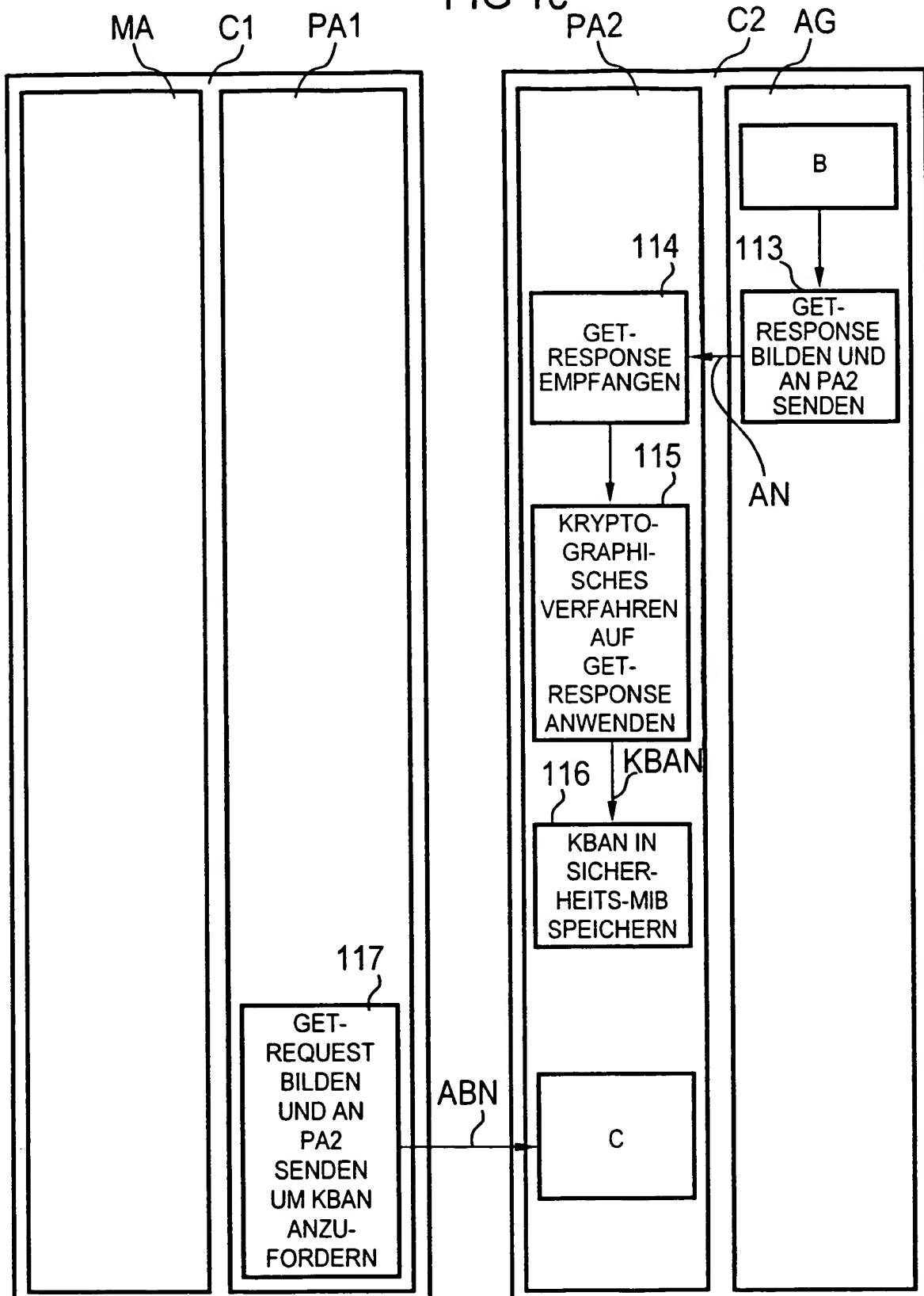
FIG 1A



2/11

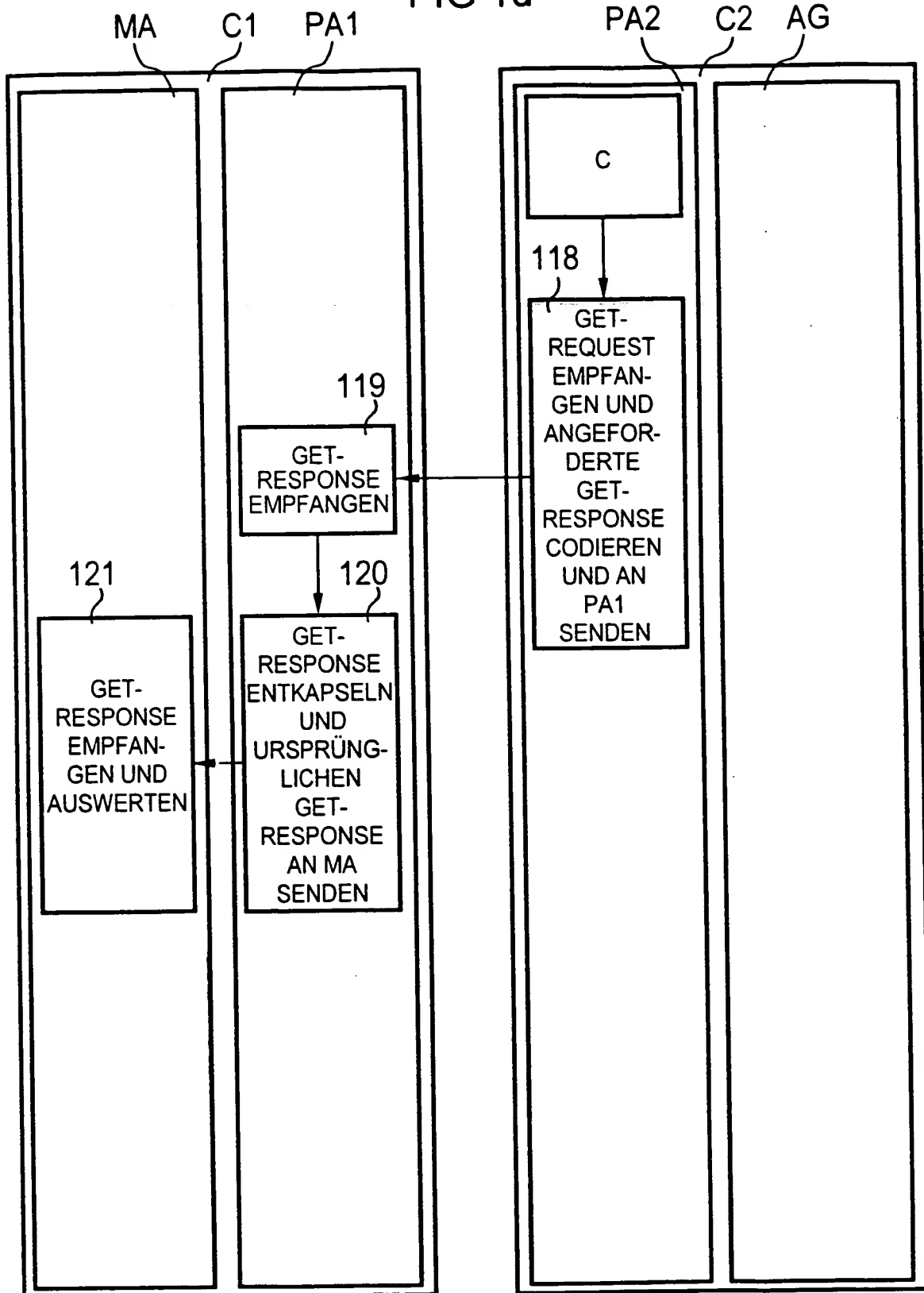
FIG 1b





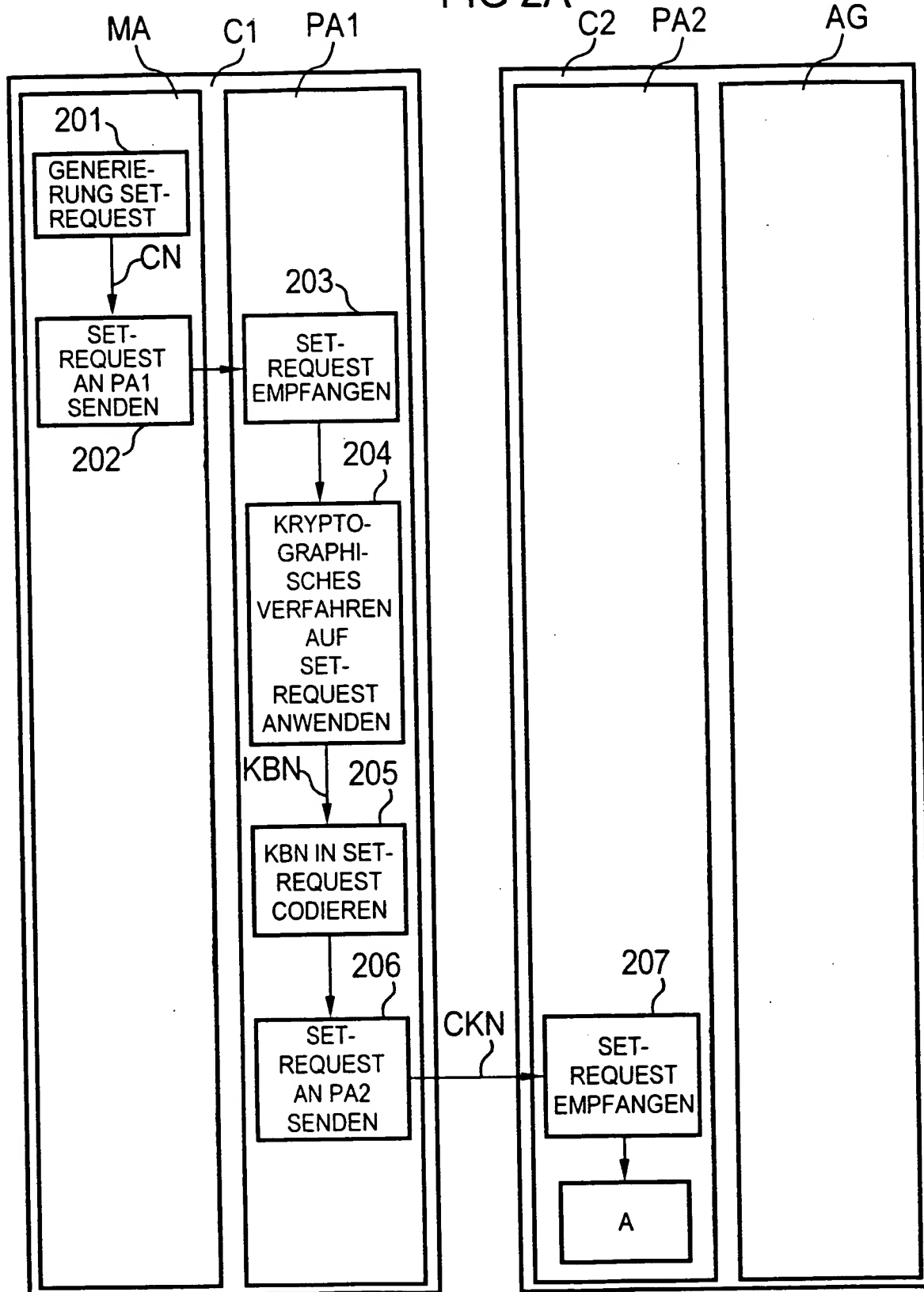
4/11

FIG 1d



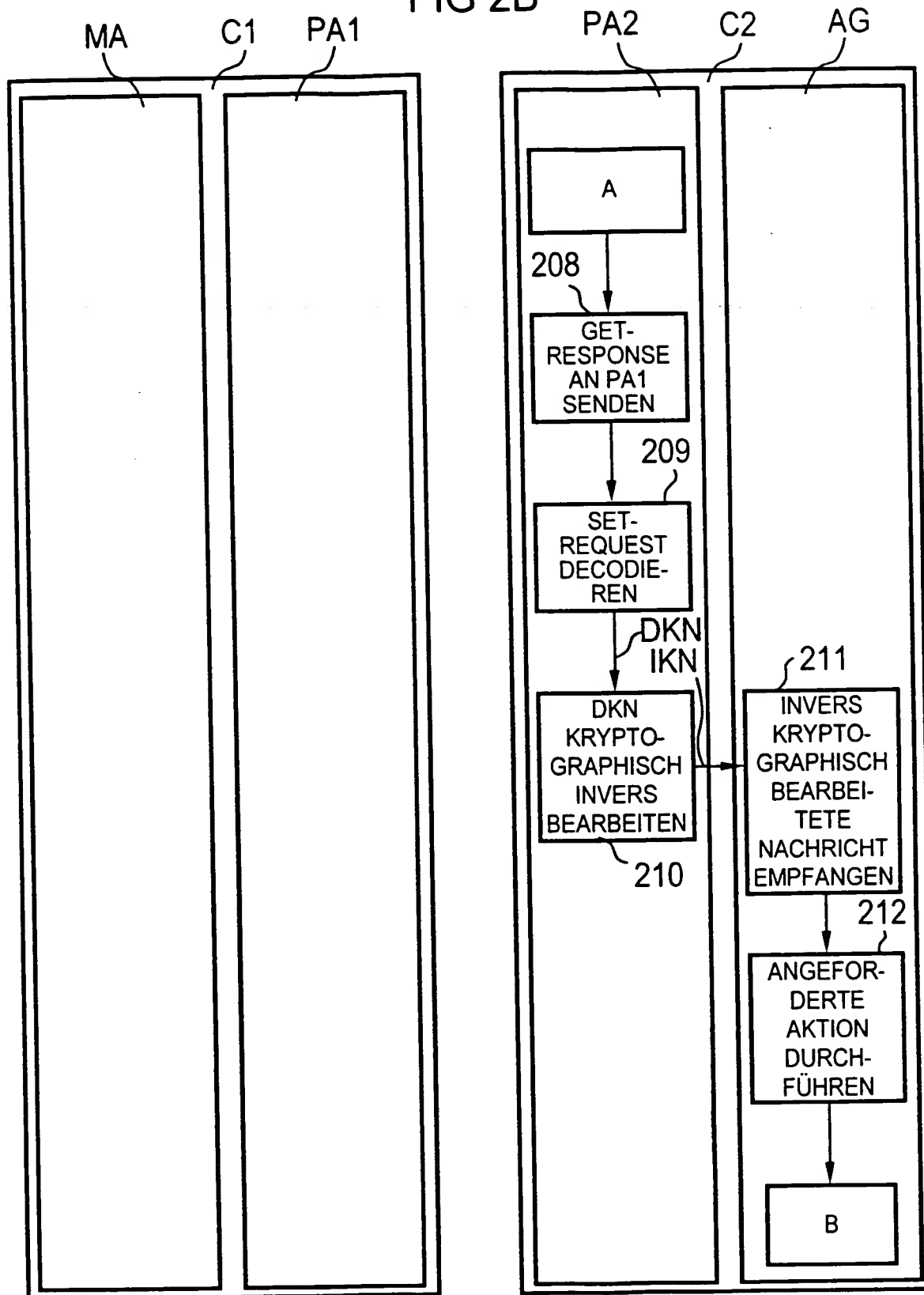
5/11

FIG 2A



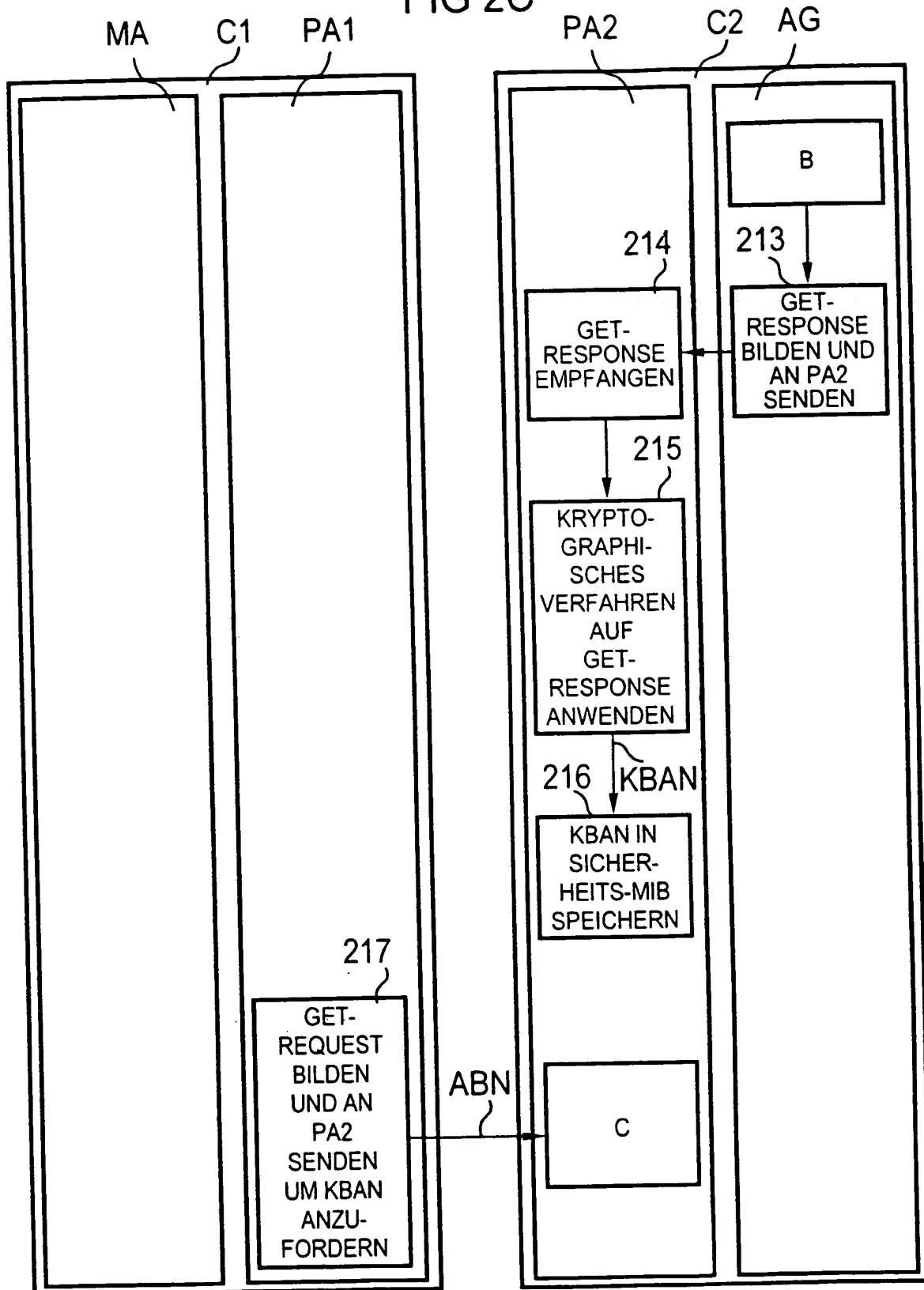
6/11

FIG 2B



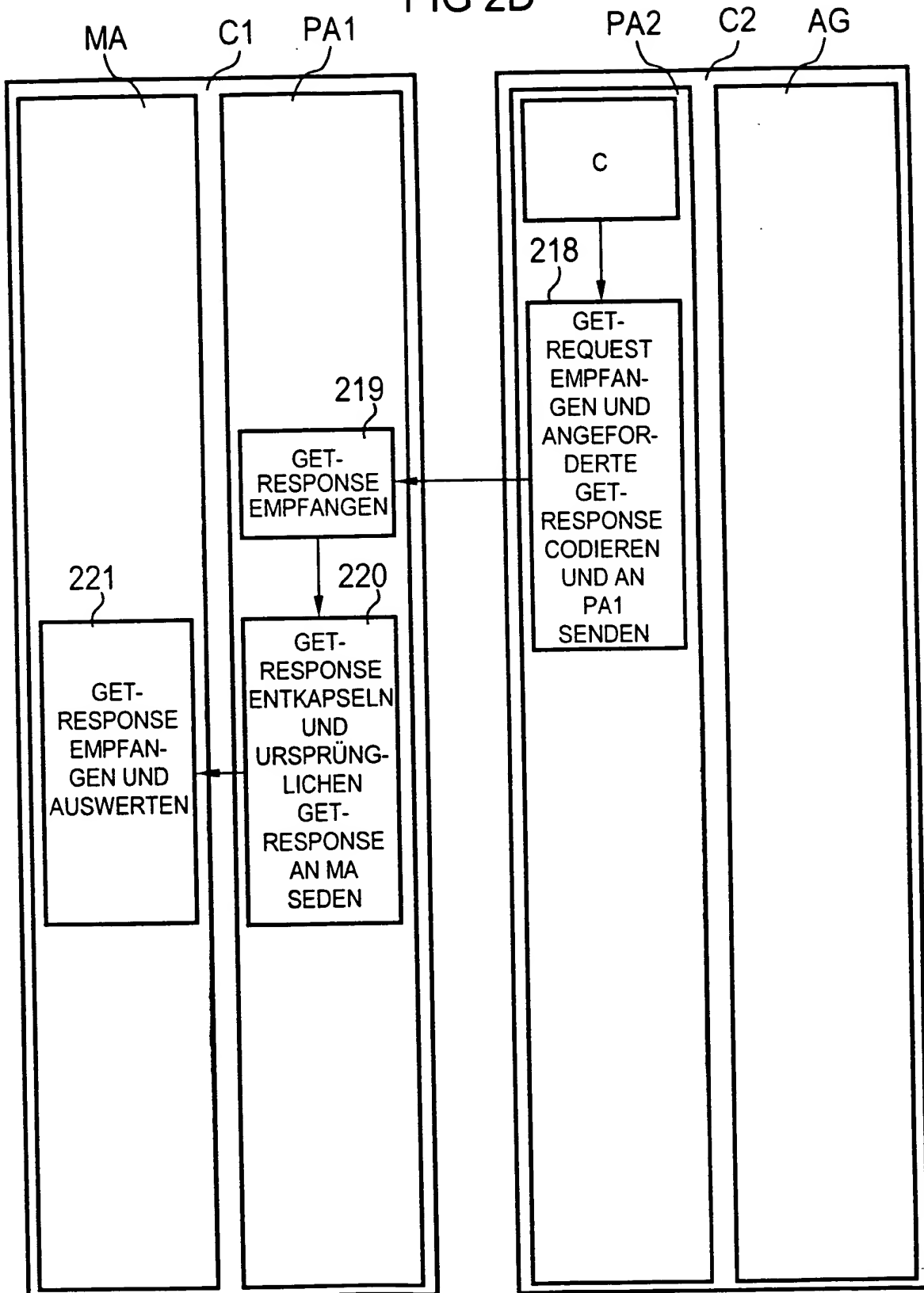
7/11

FIG 2C



8/11

FIG 2D



9/11

FIG 3

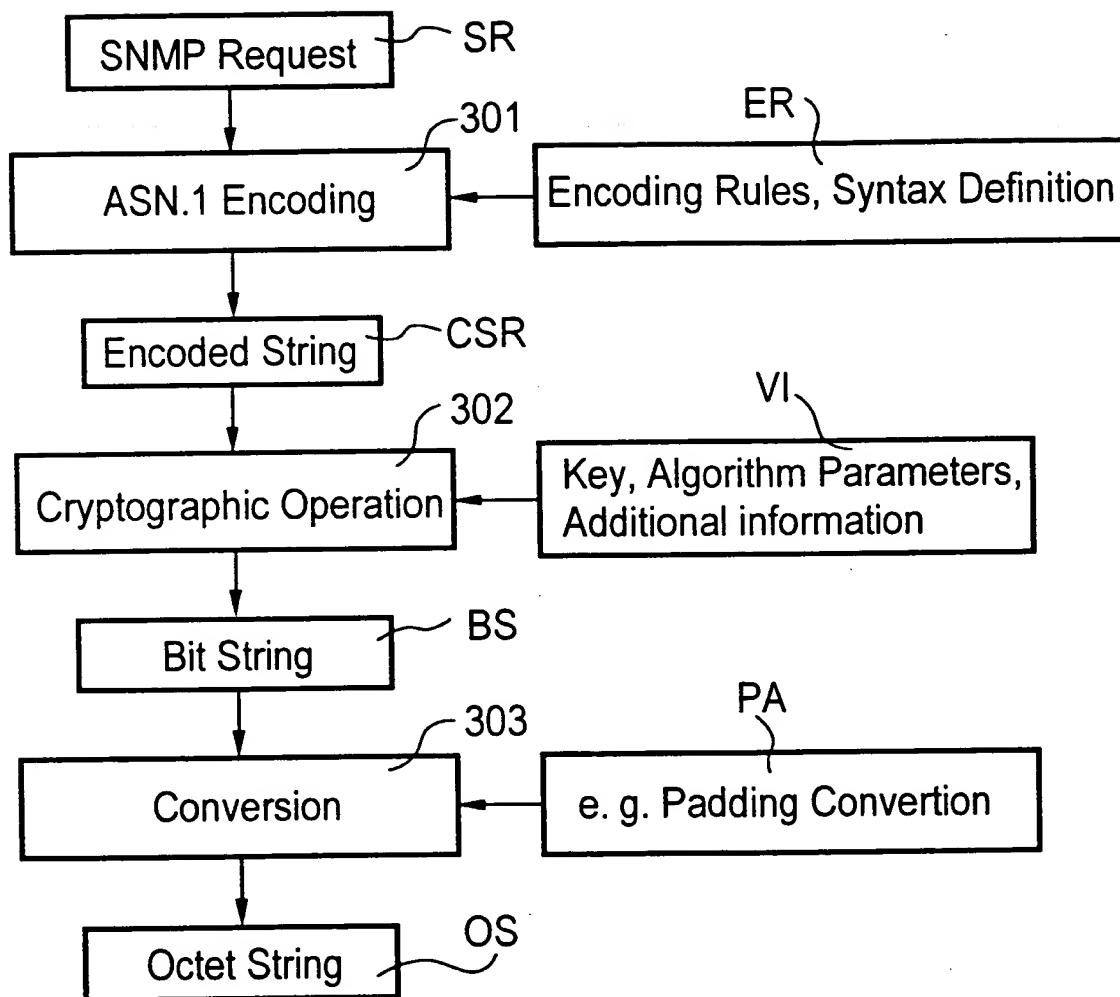


FIG 4

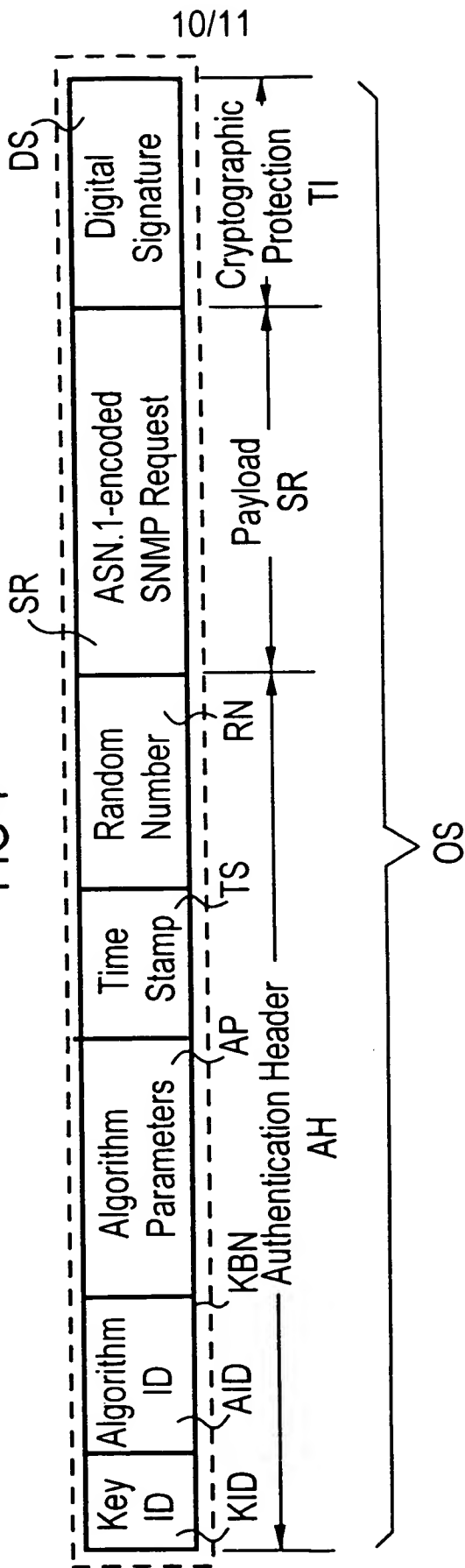
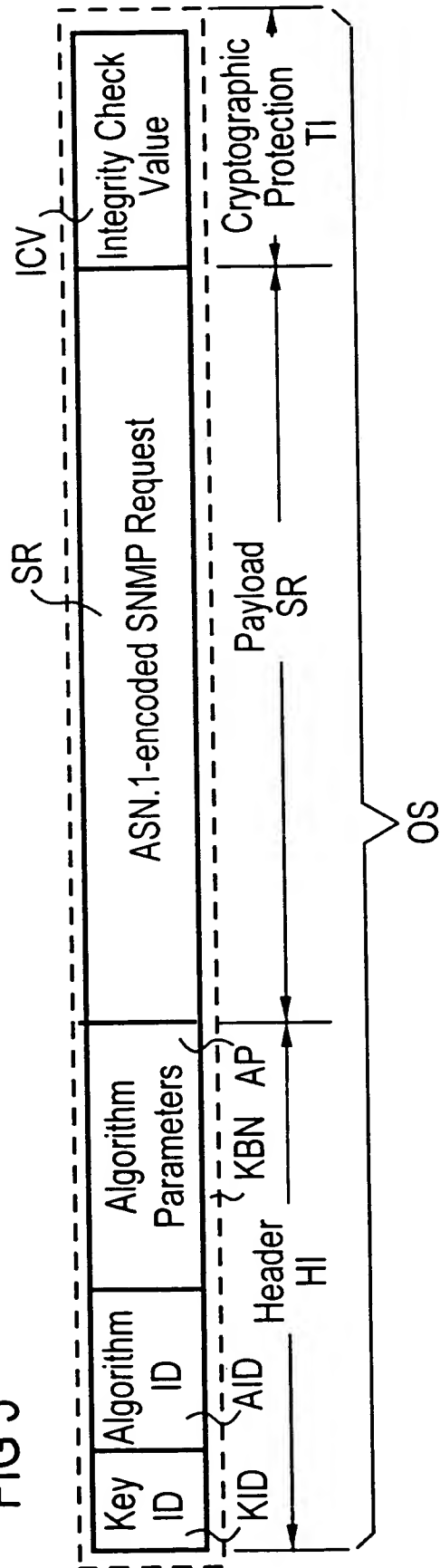
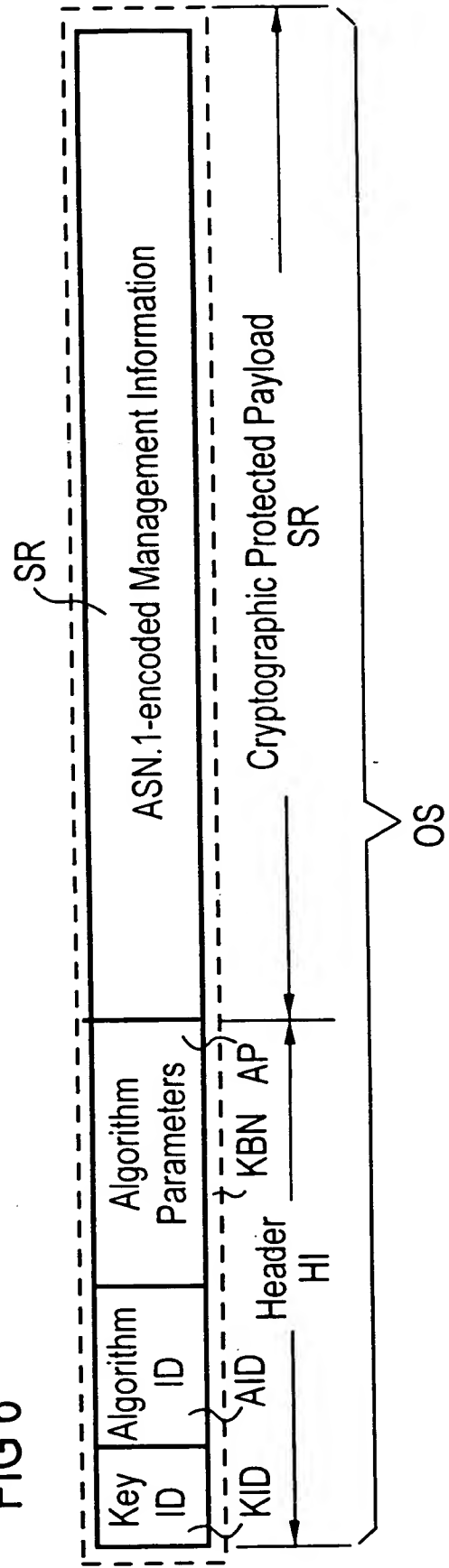


FIG 5



11/11

FIG 6



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES  
INTERNATIONALEN RECHERCHENBERICHTS  
ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

An

SIEMENS AKTIENGESELLSCHAFT  
Postfach 22 16 34  
80506 München  
GERMANY

Absendedatum  
(Tag/Monat/Jahr)

04/03/1999

Aktenzeichen des Anmelders oder Anwalts

GR 97P1798P

WEITERES VORGEHEN

siehe Punkt 1 und 4 unten

Internationales Aktenzeichen

PCT/DE 98/01693

Internationales Anmeldedatum

(Tag/Monat/Jahr)

19/06/1998

Anmelder

SIEMENS AKTIENGESELLSCHAFT et al.

1. ☒ Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

**Einreichung von Änderungen und einer Erklärung nach Artikel 19:**

Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

**Bis wann sind Änderungen einzureichen?**

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

**Wo sind die Änderungen einzureichen?**

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20.  
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a übermittelt wird.
3. ☐ **Hinsichtlich des Widerspruchs** gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß
- ☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsbüro dem Internationalen Büro übermittelt worden sind.
- ☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90 bis 90.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von **19 Monaten** seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von **20 Monaten** seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsbüro vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Theresia Van Deursen

## ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen. Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

### HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

#### Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

#### Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

#### Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

#### In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu nummerieren. Wird ein Anspruch gestrichen, so brauchen die anderen Ansprüche nicht neu nummeriert zu werden. Im Fall einer Neuenummerierung sind die Ansprüche fortlaufend zu nummerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

#### Welche Unterlagen sind den Änderungen beizufügen?

##### Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

## ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:  
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:  
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:  
"Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt." Oder "Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:  
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

### "Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigelegt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

### Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

### Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	<b>WEITERES VORGEHEN</b>	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
GR 97P1798P	Internationales Anmeldedatum (Tag/Monat/Jahr)	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr)
Internationales Aktenzeichen	19/06/1998	26/06/1997
PCT/DE 98/ 01693		
Anmelder		
SIEMENS AKTIENGESELLSCHAFT et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. ☐ Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen (siehe Feld I).
2. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).
3. ☐ In der internationalen Anmeldung ist ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt.
  - ☐ das zusammen mit der internationalen Anmeldung eingereicht wurde.
  - ☐ das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde.
  - ☐ dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
  - ☐ das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.
4. Hinsichtlich der Bezeichnung der Erfindung
  - ☐ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☒ wurde der Wortlaut von der Behörde wie folgt festgesetzt.

VERFAHREN UND COMPUTERSYSTEM ZUR CODIERUNG EINER NACHRICHT

5. Hinsichtlich der Zusammenfassung
  - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☐ wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.
6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen:
  - Abb. Nr. 1 ☒ wie vom Anmelder vorgeschlagen ☐ keine der Abb.
  - ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
  - ☐ weil diese Abbildung die Erfindung besser kennzeichnet.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
IPK 6 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie <sup>o</sup>	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X  A	DE 195 48 387 C (SIEMENS AG) 30. Januar 1997  siehe Zusammenfassung siehe Spalte 1, Zeile 64 - Spalte 2, Zeile 40 siehe Spalte 4, Zeile 47 - Spalte 5, Zeile 2 siehe Spalte 5, Zeile 23 - Spalte 7, Zeile 17 siehe Abbildung 7 --- -/--	1-6, 11-20, 25, 27 7-10, 21-24, 26



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

<sup>o</sup> Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

25. Februar 1999

Absenddatum des internationalen Recherchenberichts

04/03/1999

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Lázaro López, M.L.

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie:	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 645 912 A (IBM) 29. März 1995 siehe Zusammenfassung siehe Spalte 2, Zeile 17-52 siehe Spalte 4, Zeile 26 - Spalte 7, Zeile 5 siehe Spalte 8, Zeile 38 - Spalte 9, Zeile 38 -----	1-27

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 98/01693

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19548387 C	30-01-1997	WO 9723982 A	03-07-1997
		EP 0868804 A	07-10-1998
EP 0645912 A	29-03-1995	US 5440633 A	08-08-1995
		JP 2610107 B	14-05-1997
		JP 7087116 A	31-03-1995
		US 5524052 A	04-06-1996

# PATENT COOPERATION TREATY

**PCT**

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark  
Office  
(Box PCT)  
Crystal Plaza 2  
Washington, DC 20231  
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year)

10 February 1999 (10.02.99)

International application No.

PCT/DE98/01693

Applicant's or agent's file reference

GR 97P1798P

International filing date (day/month/year)

19 June 1998 (19.06.98)

Priority date (day/month/year)

26 June 1997 (26.06.97)

Applicant

CAPELLARO, Christoph et al

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

22 January 1999 (22.01.99)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was



was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Aino Metcalfe

Telephone No.: (41-22) 338.83.38

2766  
09/ 446425  
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

TC 2700 MAIL ROOM

APR 21 2000

RECEIVED

Applicant's or agent's file reference GR 97P1798P	<b>FOR FURTHER ACTION</b> See Notification of Transmitted of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE98/01693	International filing date (day/month/year) 19 June 1998 (19.06.1998)	Priority date (day/month/year) 26 June 1997 (26.06.1997)
International Patent Classification (IPC) or national classification and IPC H04L 9/00		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of \_\_\_\_\_ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 22 January 1999 (22.01.1999)	Date of completion of this report 07 October 1999 (07.10.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer  Telephone No. 49-89-2399-0

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE98/01693

## I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

☐ the international application as originally filed.

☒ the description, pages 1-27, as originally filed,  
pages \_\_\_\_\_, filed with the demand,  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_,  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_.

☒ the claims, Nos. 1-27, as originally filed,  
Nos. \_\_\_\_\_, as amended under Article 19,  
Nos. \_\_\_\_\_, filed with the demand,  
Nos. \_\_\_\_\_, filed with the letter of \_\_\_\_\_,  
Nos. \_\_\_\_\_, filed with the letter of \_\_\_\_\_.

☒ the drawings, sheets/fig 1/11-11/11, as originally filed,  
sheets/fig \_\_\_\_\_, filed with the demand,  
sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_,  
sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_.

2. The amendments have resulted in the cancellation of:

☐ the description, pages \_\_\_\_\_

☐ the claims, Nos. \_\_\_\_\_

☐ the drawings, sheets/fig \_\_\_\_\_

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 98/01693

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Claims	1 - 11, 13 - 27	YES
	Claims	12	NO
Inventive step (IS)	Claims	1 - 11, 13 - 27	YES
	Claims	12	NO
Industrial applicability (IA)	Claims	1 - 27	YES
	Claims		NO

### 2. Citations and explanations

#### 1. Reference is made to the following documents:

D1 = DE-C-195 48 387

D2 = EP-A-0 645 912

2. The invention pertains to a method and device for coding digital information (Claims 1 and 13), a method and device for decoding digital information (Claims 2 and 14) and a method and device for coding, transmitting and decoding digital information in a computer system (Claims 3 and 15).

3. Document D1 is regarded as the closest prior art for the subject matter of Claim 1 and discloses a method for the cryptographic protection of a computer-assisted digital communication between a program and a server. In that method, a program provides information and codes the information for a transport protocol. Immediately after coding, the coded information is decoded and the decoded information is subjected to a cryptographic process via the transport protocol. The cryptographically processed

.../...

(Continuation of V.2)

information is re-coded via the transport protocol and transmitted to a server.

4. The invention is based on a different, simpler concept: the information is coded using a coding format of a network protocol to form coded information. The coded information is then subjected to a cryptographic process. The cryptographically processed information is re-coded using the coding format of the network protocol.

The coding method according to Claim 1 is distinguished from the method known from document D1 in that the decoding prior to the cryptographic process is dispensed with. Consequently, two-fold coding using the same coding format is carried out in the method according to Claim 1. This procedure is simpler, faster and therefore more efficient.

There is no suggestion to be found in D1 that the sequence of processing steps to which information is subjected could be modified and simplified, especially as D1 emphasises that this sequence of processing steps is advantageous. Nor is there any suggestion in D2 of the problem addressed by the invention, namely to find an improved process for coding or decoding information, because the problem (namely improved authentication monitoring in network management) is of a different, higher order than the problem addressed by the invention. Consequently, the subject matter of Claim 1 involves an inventive step and therefore meets the criterion specified in PCT Article 33(3).

.../...

(Continuation of V.2)

5. In the procedure according to Claim 2 for decoding information, the processing steps for coding the information are carried out in inverse order and in each case with an inverse process to that used for coding. The subject matter of independent Claim 2 therefore involves an inventive step and hence meets the criterion specified in PCT Article 33(3).
6. Independent Claim 3 relates to a method for coding information according to Claim 1, for transmitting the information from a first computer unit to a second computer unit and for decoding information according to Claim 2. Consequently, the subject matter of Claim 3 involves an inventive step (PCT Article 33(3)).
7. Claims 4 to 11 are dependent on Claims 1, 2 or 3, and therefore they, too, meet the requirements of the PCT with regard to novelty and inventive step.
8. Independent Claim 12 relates only to a device comprising a computer unit and contains no additional technical feature (see Box VIII). The subject of this claim is therefore not novel (PCT Article 33(2)).
9. Independent Claims 13 to 15 include the device features corresponding to process Claims 1 to 3 and therefore they, too, meet the requirements of the PCT with regard to novelty and inventive step.
10. Claims 16 to 27 are dependent on Claims 13, 14 or 15 and therefore they, too, meet the requirements of the PCT with regard to novelty and inventive step.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 98/01693

## VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. The description did not cite document D1 and did not indicate the relevant prior art disclosed therein, in contravention of the requirements of PCT Rule 5.1(a)(ii).
2. The features of the claims are not followed by reference signs placed between parentheses (PCT Rule 6.2(b)).
3. Independent Claims 1, 2, 3, 13, 14 and 15 have not been worded in the two-part form according to PCT Rule 6.3(b). In the present case, however, the two-part formulation seems appropriate. Consequently, the features which, in combination, are known from the prior art (document D1) should be incorporated in a preamble (PCT Rule 6.3(b)(i)) and the other features should be specified in a characterizing portion (PCT Rule 6.3(b)(ii)).

The applicants have not given any reasons as to why these claims should not have the two-part formulation. Furthermore, they have not clearly indicated in the description which features of the subjects of Claims 1, 2, 3, 13, 14 and 15 are already known from document D1; see PCT Preliminary Examination Guidelines PCT/GL/3, Ch. III, 2.3a.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 98/01693

## VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claim 12 does not comply with the requirements of PCT Article 6 in conjunction with PCT Rule 6.3:

Claim 12 is, despite its reference to other claims, an independent claim. According to PCT Rule 6.3, every independent claim must contain all the essential technical features necessary for the definition of the invention, that is, the meaning of every independent claim must be clear from the wording of the claim alone (without reference to other independent claims). Claim 12 should therefore contain technical features of a device.

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

REC'D 12 OCT 1999

WIPO PCT

### INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)



Aktenzeichen des Anmelders oder Anwalts GR 97P1798P	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE98/01693	Internationales Anmeldedatum (Tag/Monat/Jahr) 19/06/1998	Prioritätsdatum (Tag/Monat/Jahr) 26/06/1997
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/00		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.
  - ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags  22/01/1999	Datum der Fertigstellung dieses Berichts  07. 10. 99
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter  Cretaine, P  Tel. Nr. +49 89 2399 8828 

**I. Grundlage des Berichts**

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

**Beschreibung, Seiten:**

1-27                      ursprüngliche Fassung

**Patentansprüche, Nr.:**

1-27                      ursprüngliche Fassung

**Zeichnungen, Blätter:**

1/11-11/11              ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung,        Seiten:  
☐ Ansprüche,            Nr.:  
☐ Zeichnungen,        Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

**V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

**1. Feststellung**

Neuheit (N)	Ja: Ansprüche	1-11, 13-27
	Nein: Ansprüche	12
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-11, 13-27
	Nein: Ansprüche	12
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-27
	Nein: Ansprüche	

**2. Unterlagen und Erklärungen**

**siehe Beiblatt**

**VII. Bestimmte Mängel der internationalen Anmeldung**

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

**siehe Beiblatt**

**VIII. Bestimmte Bemerkungen zur internationalen Anmeldung**

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

**siehe Beiblatt**

**Zu Punkt V**

**Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

1. Es wird auf die folgenden Dokumente verwiesen:

D1 = DE-C-195 48 387

D2 = EP-A-0 645 912

2. Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Codierung einer digitalen Nachricht (Ansprüche 1 und 13), ein Verfahren und eine Vorrichtung zur Dekodierung einer digitalen Nachricht (Ansprüche 2 und 14), sowie ein Verfahren und eine Vorrichtung zur Codierung, Übertragung und Dekodierung einer digitalen Nachricht in einem Computersystem (Ansprüche 3 und 15).
3. Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen und offenbart ein Verfahren zur kryptographischen Sicherung einer rechnergestützten digitalen Kommunikation zwischen einem Programm und einer Benutzereinheit. Bei diesem Verfahren wird von einem Programm eine Nachricht gebildet und die Nachricht für ein Transportprotokoll codiert. Direkt nach der Codierung wird unter Verwendung des Transportprotokolls die codierte Nachricht wieder decodiert und die decodierte Nachricht einem kryptographischen Verfahren unterzogen. Danach wird die kryptographisch bearbeitete Nachricht wiederum mit dem Transportprotokoll codiert und an eine Benutzereinheit übertragen.
4. Die Erfindung geht von einem anderen, einfacheren Ansatz aus: die Nachricht wird unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert. Anschließend wird die codierte Nachricht einem kryptographischen Verfahren unterzogen. Die kryptographisch bearbeitete Nachricht wird unter Verwendung des Codierungsformats des Netzwerkprotokolls ein weiteres Mal codiert.

Das Codierungsverfahren gemäß Anspruch 1 unterscheidet sich von dem aus dem Dokument D1 bekannten Verfahren dadurch, daß die Dekodierung vor dem kryptographischen Verfahren entfällt. Deshalb erfolgt bei dem Verfahren gemäß Anspruch 1 eine zweifache Codierung unter Verwendung des gleichen Codierungsformats. Diese Vorgehensweise ist einfacher, schneller und damit effizienter.

In D1 ist kein Hinweis darauf zu finden daß die Abfolge von Bearbeitungsschritten, denen eine Nachricht unterzogen wird, geändert und vereinfacht werden könnte, zumal gerade diese Abfolge von Bearbeitungsschritten in D1 als vorteilhaft herausgestellt wird. In D2 ist auch kein Hinweis auf die Aufgabe der Erfindung, nämlich eine verbesserte Codierung bzw. Decodierung einer Nachricht, zu finden, da die Aufgabe (nämlich eine verbesserte Authentizitätsüberprüfung im Rahmen einer Verwaltung eines Netzwerks) eine andere, übergeordnete Ebene als die Aufgabe der Erfindung betrifft. Der Gegenstand des Anspruchs 1 beruht somit auf einer erfinderischen Tätigkeit und erfüllt damit das in Artikel 33(3) PCT genannte Kriterium.

5. Bei der Vorgehensweise gemäß Anspruch 2 zur Dekodierung einer Nachricht werden die Bearbeitungsschritte bei der Codierung der Nachricht in umgekehrter Reihenfolge und mit jeweils einem zu dem bei der Codierung verwendeten inversen Verfahren durchgeführt. Der Gegenstand des unabhängigen Anspruchs 2 beruht somit auf einer erfinderischen Tätigkeit und erfüllt damit das in Artikel 33(3) PCT genannte Kriterium.
6. Der unabhängige Anspruch 3 bezieht sich auf ein Verfahren zur Kodierung einer Nachricht gemäß Anspruch 1, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Dekodierung einer Nachricht gemäß Anspruch 2. Deshalb beruht der Gegenstand des Anspruchs 3 auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).
7. Die Ansprüche 4 bis 11 sind von Ansprüchen 1, 2 oder 3 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

8. Der unabhängige Anspruch 12 bezieht sich lediglich auf eine Vorrichtung mit einer Recheneinheit und enthält kein weiteres technisches Merkmal (siehe Punkt VIII). Der Gegenstand dieses Anspruchs ist daher nicht neu (Artikel 33(2) PCT).
9. Die unabhängigen Ansprüche 13 bis 15 enthalten die den Verfahrensansprüche 1 bis 3 entsprechenden Vorrichtungsmerkmale und erfüllen damit ebenfalls die Erfordernisse des PCT in Bezug auf Neuheit und erfinderische Tätigkeit.
10. Die Ansprüche 16 bis 27 sind von Ansprüchen 113, 14 oder 15 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in Bezug auf Neuheit und erfinderische Tätigkeit.

#### **Punkt VII**

#### **Bestimmte Mängel der internationalen Anmeldung**

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in dem Dokument D1 offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.
2. Die Merkmale der Ansprüche sind nicht mit in Klammern gesetzten Bezugszeichen versehen worden (Regel 6.2 b) PCT).
3. Die unabhängigen Ansprüche 1, 2, 3, 13, 14 und 15 sind nicht in der zweiteiligen Form nach Regel 6.3 b) PCT abgefaßt. Im vorliegenden Fall erscheint die Zweiteilung jedoch zweckmäßig. Folglich sollten die in Verbindung miteinander aus dem Stand der Technik bekannten Merkmale (Dokument D1) in einem Oberbegriff zusammengefaßt (Regel 6.3 b) i) PCT) und die übrigen Merkmale in einem kennzeichnenden Teil aufgeführt werden (Regel 6.3 b) ii) PCT).

Der Anmelder hat keine Gründe dafür genannt, warum diese Ansprüche nicht die zweiteilige Form haben sollten. Ferner hat er in der Beschreibung nicht klar

angegeben, welche Merkmale der Gegenstände der Ansprüche 1, 2, 3, 13, 14 und 15 bereits aus dem Dokument D1 bekannt sind; siehe die PCT-Richtlinien PCT/GL/3 III, 2.3a.

**Zu Punkt VIII**

**Bestimmte Bemerkungen zur internationalen Anmeldung**

Anspruch 12 entspricht nicht den Erfordernissen des Artikels 6 PCT in Verbindung mit Regel 6(3) PCT:

Der Anspruch 12 ist, trotz seiner Bezugnahme auf andere Patentansprüche, ein unabhängiger Anspruch. Gemäß Regel 6(3) PCT hat jeder unabhängige Anspruch die für die Festlegung des Gegenstandes des Schutzbegehrens notwendigen wesentlichen technischen Merkmale der Erfindung zu enthalten, d.h. jeder unabhängige Anspruch muß mit seinem Wortlaut aus sich heraus (ohne Rückbeziehung auf andere selbständige Ansprüche) verständlich sein. Anspruch 12 sollte deshalb technische Merkmale einer Vorrichtung enthalten.